分 类 号 _____ 密　　级 _____

U　D　C _____ 单位代码 10151

大　连　海　事　大　学

硕士学位论文

抗矿池集中化的共识机制研究

杨超智

指 导 教 师	李志淮	职　　称	教授
学位授予单位	大连海事大学		
申请学位级别	工学硕士	学科（专业）	计算机科学与技术
论文完成日期	2017 年 12 月	答辩日期	2018 年 3 月

答辩委员会主席 _____

Research on Consensus Mechanism for Anti - mining Concentration

A thesis Submitted to

Dalian Maritime University

In partial fulfillment of the requirements for the degree of

Master of Academic

by

Yang Chaozhi

(Computer Science and Technology)

Thesis Supervisor: Professor Li Zhihuai

March 2018

大连海事大学学位论文原创性声明和使用授权说明

原创性声明

本人郑重声明：本论文是在导师的指导下,独立进行研究工作所取得的成果，撰写成博/硕士学位论文 “抗矿池集中化的共识机制研究”。除论文中已经注明引用的内容外，对论文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本论文中不包含任何未加明确注明的其他个人或集体已经公开发表或未公开发表的成果。本声明的法律责任由本人承担。

学位论文作者签名：_____

学位论文版权使用授权书

本学位论文作者及指导教师完全了解大连海事大学有关保留、使用研究生学位论文的规定，即：大连海事大学有权保留并向国家有关部门或机构送交学位论文的复印件和电子版，允许论文被查阅和借阅。本人授权大连海事大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，也可采用影印、缩印或扫描等复制手段保存和汇编学位论文。同意将本学位论文收录到《中国优秀博硕士学位论文全文数据库》（中国学术期刊（光盘版）电子杂志社）、《中国学位论文全文数据库》（中国科学技术信息研究所）等数据库中，并以电子出版物形式出版发行和提供信息服务。保密的论文在解密后遵守此规定。

本学位论文属于： 保 密□ 在_____年解密后适用本授权书。

不保密□ （请在以上方框内打“√” ）

论文作者签名： **导师签名：**

日期： 年 月 日

摘　　要

传统的集中模式，数据信息均由中心化服务器统一管理，因此导致了可靠性与可信性问题。而区块链技术有效地解决了上述这些问题。但是在区块链技术的发展过程中还存在很多不足。例如比特币使用的 POW 共识机制的缺陷就被利益集团所利用。利益集团建立了矿池并垄断了的算力和区块铸造权。这种行为违背了区块链技术的初衷，同时也使得区块链网络存在着遭受 51%攻击的风险。矿池集中化问题已经成为了制约区块链技术发展的主要问题。

本文在分析现有了区块链共识机制的基础上，提出了一种基于权益调节的工作量证明机制 POWS。POWS 共识机制的核心思想就是在 POW 共识机制中引入了币龄的概念，用以调节不同节点的挖矿难度。POWS 共识机制通过算力和币龄两个因素来调节挖矿难度。在单个因素大量聚集时，POWS 共识机制降低了算力或币龄对出块效率的影响。POWS 共识机制降低了矿池对普通节点的利益驱动。同时算力和币龄两个影响因素也会增加矿池运营的成本。

本文从基本性能和抵御矿池能力两个方面，对 POWS 共识机制与 POW 共识机制及 POS 共识机制进行了对比实验。实验结果表明，POWS 共识机制能够满足正常的区块链系统的性能需求，同时在较好的降低了算力或币龄对区块生成效率的影响、缩小了矿池节点和非矿池节点的出块效率差距、降低了矿池对非矿池节点的利益驱动。

关键词：区块链；共识机制；矿池集中化；POW；POS；POWS

ABSTRACT

The traditional centralized mode, data and information are centrally managed by the centralized server, thus leading to the reliability and credibility issues. The blockchain technology effectively solves these problems. However, there are still many shortcomings in the development of blockchain technology. For example, the drawbacks of the POW consensus mechanism used by bitcoin are exploited by interest groups. Interest groups set up the mining pool and monopolized the power and block casting rights. This behavior runs counter to the original intention of blockchain technology, but also exposes the blockchain network to a 51% risk. The problem of pool concentration has become the main problem restricting the development of blockchain technology.

Based on the analysis of the existing consensus mechanism of blockchain, this paper proposes a POWS mechanism based on the adjustment of workload. The core idea of POWS consensus mechanism is to introduce the concept of currency age into POW consensus mechanism to adjust the difficulty of mining different nodes. POWS consensus mechanism adjusts the difficulty of mining by calculating the power and currency age. The POWS Consensus Mechanism reduces the impact of counting power or currency age on the efficiency of block-outs when a single factor accumulates in large numbers. The POWS Consensus Mechanism reduces the profit-driven nature of the mine pool to common nodes. At the same time, the computing power and currency age two factors will also increase the cost of mining operations.

This article compares the POWS consensus mechanism with the POW and the POS consensus mechanism from the aspects of basic performance and resistance to mine pool. The experimental results show that the POWS consensus mechanism can meet the performance requirements of normal blockchain systems and reduce the effect of calculating power or currency age on the block generation efficiency and reducing the gap in the efficiency of block production between mine pool nodes and reducing the profit drive of the mine pool to non-mine pool nodes.

Key Words：Blockchain; Consensus Mechanism; Mining Pool Concentration; POW; POS; POWS

目　录

第 1 章 绪论

1.1 研究背景

近年来区块链技术逐渐成为了学界和商界研究讨论的热点话题。区块链技术的实质就是基于 P2P 网络的分布式记账技术。区块链技术最初被应用于去中心化的比特币电子现金交易系统[1]，其最主要特点是去中心化与去信任化。

传统的中心化服务器模式存在着很多的弊端，可靠性、可用性和可信性均得不到保障。传统的中心化服务器在物理上保存于一个或若干个场地，很容易遭受到 DDOS 攻击。而区块链应用系统没有中心化服务器，或者说区块链网络中的所有全节点都是服务器。这样区块链应用系统的数据信息就存储于全球各地的数以亿计的主机之中，很难遭受到攻击。在传统模式中所有数据信息都集中存储于中心化服务器，数据篡改以及数据泄露成为及其容易发生的事情。而区块链网络中的数据信息存储于所有完全节点的硬盘中并且是加密的，数据一旦被部分节点所篡改也能够发现且不被承认。传统的集中模式中节点之间是不平等，而区块链技术中所有节点都是平等的关系，不存在任何中心节点。所有独立平等的节点依据事先在程序中定义好的版本协议，达成整个区块链网络的共识。

区块链技术发展迅速，但自身的缺陷依然很多，距离成为一项惠及全球民众的成熟应用技术还差很远。区块链技术发展的初期是区块链技术 1.0 时代[2]，主要是以比特币为代表的数字加密货币交易系统。目前区块链技术已经进入了区块链技术 2.0 时代，主要是以以太坊[3]为代表的智能合约应用平台[4]。区块链技术正在向区块链技术 3.0 时代探索，不久的将来将区块链技术将应用于社会各行各业。

区块链技术的第一个实际应用就是比特币系统 Bitcoin 简称 BTC，一种点对点的电子现金交易系统[5]，首次见于中本聪于 2008 年发表的《Bitcoin:A Peer-to-Peer Electronic Cash System》一文。比特币系统作为第一个区块链应用已经成为了区块链技术的代名词[6]。因为比特币系统是第一个区块链应用，其本身在技术上也最原始、最不完善、存在着诸多先天缺陷[7]。其中最为危险与严重的技术缺陷就是共识机制本身容易造成人为的矿池中心化问题[8]。这已经违背了区块链技术的初衷，成为了掣肘区块链技术发展的主要问题。

区块链技术的核心技术之一就是共识机制技术[9]。共识机制解决在点对点网络中的可信通信问题，即拜占庭将军问题。简而言之，对于区块链技术来说共识机制就是决定由谁来产生新区块、记录数据信息并维持整个区块链网络一致性的问题。在公有区块链应用中主要的共识机制有两大类，一类是 POW 共识机制[10]，另一类是 POS 共识机制[11]。POW 共识机制会人为地产生算力集中化的矿池，POS 共识机制会产生币龄集中化的矿池。因此完善共识机制就是解决矿池集中化的首要方法。

1.2 国内外研究现状

1.2.1 区块链共识机制研究现状

区块链技术第一次出现于比特币系统之中。区块链技术是比特币系统的底层基础架构，是从比特币系统中总结与发展出来的一种新兴互联网技术。区块链技术以 P2P 网络作为底层网络架构，以非对称加密算法如椭圆曲线加密算法 [12]生成公钥与私钥，以散列哈希算法如 SHA256 算法[13]对交易信息及区块梅克尔树[14]进行不可逆的加密，以共识机制如 POW 工作量证明机制维护区块链的数据一致性、去中心化以及去信任化等。区块链技术最核心的技术就是共识机制。

区块链技术主要有三个应用场景：区块链公有链、区块链联盟链以及区块链私有链。其中区块链私有链和现在的分布式数据库差别不大，其具有较强的中心化以及信任化；区块链联盟链也主要应用于企业、行业之间，也具有一定的中心化以及信任化。区块链私有链以及区块链联盟链都不是本文要研究的内容，本文主要研究的是区块链公有链。以比特币为代表的第一代数字货币交易平台区块链和以以太坊为代表的第二代智能合约平台区块链都是公有链。区块链公有链是完全的去中心化以及去信任化。区块链公有链实现去中心化以及去信任化特性的主要依仗就是共识机制。

自从区块链技术诞生以来，大大小小的新区块链公有链应用系统也出现了成千上万个。共识机制也由最初的 POW 工作量证明机制发展出了几十种共识机制。这几十种区块链共识机制大体上可以划分成两大类，一类是 POW 工作量证明机制、另一类是 POS 权益证明机制。POW 工作量证明机制作为最经典的区块链共识

机制，在区块链发展的初期受到了大家的热捧，出现了很多模仿 POW 工作量证明机制的区块链应用系统。但是随着时间的推移、随着区块链技术的不断的发展，POW 工作量证明机制其本身所具有的消耗大量算力以及电力、浪费能源以及资源、出块时间长、抗并发性差、算力无限制增大导致挖矿难、矿池集中算力以及绑架算力等缺点日益突出，日益受到人们的担忧。尤其是最后一点，矿池大肆集中算力以及绑架算力已经严重危害了区块链去中心化以及去信任化的初衷[15]。以比特币系统为例，几个主要的大矿池分别控制了比特币系统全网总算力的 5%到 35%，使比特币系统始终面临着受到 51%攻击的风险[16]。最近半年特别火爆的比特币几次分叉事件就是各大矿池主导的结果。因此，矿池集中算力的这种现象已经影响了区块链应用系统的公平性、危害了区块链应用系统的去中心化以及去信任化、掣肘了区块链技术的正常发展。为此，众多研究学者为了应对矿池、算力与电力消耗、区块产生速度慢等问题，推出了 POS 权益证明机制。

POS 权益证明机制的主要思想就是持有币本身会产生利息，产生新的币。币的持有者通过清空币龄来产生区块，币龄较大的区块链地址具有较大的概率获得铸造新区块的权利。第一个使用 POS 权益证明机制的区块链应用点点币系统使用的是币龄概念，之后也存在一些其他的 POS 区块链应用系统使用单纯的币的概念。POS 权益证明机制解决了算力以及电力消耗的问题，区块产生时间也大大缩短，但是在针对矿池问题的方面并没有得到很好的解决。POS 权益证明机制的挖矿不需要太多的算力，算力的大小也不影响获得新的区块铸造权的可能性，但是其却产生了一种新的垄断新区块铸造权的方式——数字货币集中化。从算力集中化到数字货币的集中化，垄断新的区块铸造权的本质并没有发生变化，使用 POS 权益证明机制的区块链应用系统反而会更加容易分叉，同时普通矿工节点生成新的区块的公平性更低了。

POW 工作量证明机制以及 POS 权益证明机制都不能很好地解决矿池集中挖矿资源的问题，于是研究人员就提出了 POW+POS 的混合共识机制的想法。目前主流的混合共识机制主要想法有四种：第一种是前期使用 POW 工作量证明机制，到一定区块数目后再切换为 POS 权益证明机制；第二种是 POW 工作量证明机制和 POS 权益证明机制依次轮流切换使用；第三种是 POW 工作量证明机制和以太

坊的 Casper 押注共识机制相结合的共识模式；第四种是 POW 工作量证明机制和量子链的 MPOS 互惠共识机制相结合的区块链共识模式。但是这四种技术方案，第一种没有完全解决问题，第二种目前还没有实际项目应用，第三种还在孵化之中尚未切换到以太坊主网使用，且以太坊官方没有公布具体技术细节，第四种刚刚应用于量子链系统没有多久，实际效果尚未得到验证，且量子链官方同样没有公布技术细节。

1.2.2 区块链技术应用系统研究现状

区块链技术的第一个实际应用系统是比特币系统，实际上区块链技术也是在比特币系统中被首次提炼、整理后提出的。《区块链世界》一书中曾经提到区块链技术的发展规划与畅想主要分为三个阶段，区块链技术 1.0 数字货币交易、区块链技术 2.0 智能合约平台、区块链技术 3.0 区块链社会分工与合作。

区块链技术 1.0 主要是数字货币交易平台的发展阶段，主要是与转账、汇款、数字化支付相关的区块链应用系统。区块链技术 1.0 的应用系统主要使用的是 POW 工作量证明机制，以比特币为代表，主要有比特币、莱特币、达世币等待。区块链技术 2.0 主要是智能合约平台的发展阶段[17]，主要是应用于股票、产权、智能财产、抵押、物流溯源、防伪、云存储、游戏、市场预测、能源、医疗、社交网络等各方面。区块链技术 2.0 的应用系统主要使用的是 POS 权益证明机制和 POW 工作量证明机制，以以太坊为代表，主要有比特股、量子链、Zasch 等。区块链技术 3.0 阶段目前还未到来，其将是超越数字货币、金融和市场的区块链应用，区块链技术将广泛应用于社会各行业。目前区块链技术的发展正处于区块链技术 2.0 阶段，区块链应用系统百花齐放，在各行各业都开始尝试应用，虽然各种区块链应用系统还处于不成熟的阶段，但是随着区块链技术的不断发展与完善，区块链技术终将发展到区块链技术 3.0 阶段[18]。

1.3 论文的主要研究内容

本文在研究分析现有的共识机制的基础上，提出了一种 POW+POS 的混合共识机制，即基于权益调节的工作量证明机制(Proof of Work Based on Adjusted Stake)，

简称 POWS。POWS 共识机制的设计宗旨是抵御矿池集中化、有效地增加矿池运营成本、减弱矿池对普通矿工节点的利益驱动。

本文实现了 POWS 共识机制及其区块链共识机制。在实验室环境下对 POWS 共识机制、POW 共识机制、POS 共识机制进行了基本性能和抵御矿池的对比实验。实验结果表明 POWS 共识机制能够满足正常的区块链系统的性能需求、较好地减弱了算力与币龄对区块产生效率的影响、并减弱了矿池对普通节点的利益驱动。

1.4 论文的章节安排

根据研究内容对本文的章节规划如下：

第 1 章 绪论：本章阐述了本文的研究背景。分析了区块链技术发展的国内外研究现状、介绍了本文的研究内容。最后介绍了本文的章节安排。

第 2 章 区块链相关技术介绍。本章主要介绍与研究内容相关的技术。介绍了区块链技术的结构、原理和共识机制。

第 3 章 对现有共识机制进行分析。分析了各种共识机制的优缺点以及矿池集中化的状况。

第 4 章 基于权益调节的工作量证明机制的设计与实现。本章主要阐述了 POWS 共识机制及共识机制的设计与实现。

第 5 章 实验与分析。在实验室环境下，对 POWS 共识机制与 POW 共识机制、POS 系统进行对比实验。

第 6 章 总结与展望。对论文做出了总结，对下一步研究工作进行了展望。

第 2 章 相关技术介绍

2.1 区块链技术

2008 年区块链技术在全球爆发信任危机的背景下应运而生[19]。区块链技术一经面世就受到了商业领域与研究人员的热捧[20]。除了以比特币、以太坊等为代表的众多公有区块链项目外，各个国家、各大公司、各大组织也都在积极的推进区块链技术的发展、开发孵化区块链项目[21]。超级账本项目[22]是由 Linux 基金会于 2015 年 12 月创立领导的区块链项目，其核心董事会及团队成员包括 IBM、埃森哲、英特尔、戴勒姆、Airbus、摩根大通、日立、富士通、美国运通、美国证券托管结算公司、芝加哥商品交易所等金融、物联网、航空及医疗等领域巨头企业。国内的腾讯公司也推出了区块链金融级解决方案 Baas(Blockchain as a Service)[23]，旨在建立一个灵活、安全、可靠的区块链平台以提供智能合约、数字资产交易、供应链管理、跨境清算与支付等服务。国内还开展了一些区块链技术相关的研究组织，例如金融区块链合作联盟、中国分布式总账基础协议联盟以及中国区块链研究联盟(Chain Blockchain Research Alliance)等。国务院也曾发文大力支持国内发展区块链技术。

2.2 区块链的基本结构

从广义上讲，区块链技术是一种去中心化的记录技术[24]。区块链技术也可称之为一种基于 P2P 网络的分布式总账技术[25]。区别于现有的第三方支付与清算系统的中心化记账方式[26]，区块链交易系统的记账方式是所有节点都参与每一笔交易的记账、都验证每一笔交易、都验证每一个新的记账区块的合法性[27]。区块链系统中所有节点的地位都是平等的，没有任何中心节点，所有节点一同维护整个系统的正常运行，所有节点都保存完整的区块链数据[28]。整个系统的数据一致性、安全性以及合法性都是靠共识机制实现的。整个区块链系统中的节点不需要信任系统中的任何一个节点，就能使得系统正常、安全、可靠的运行。

去中心化的记账方式和中心化的记账方式如图 2.1 所示。

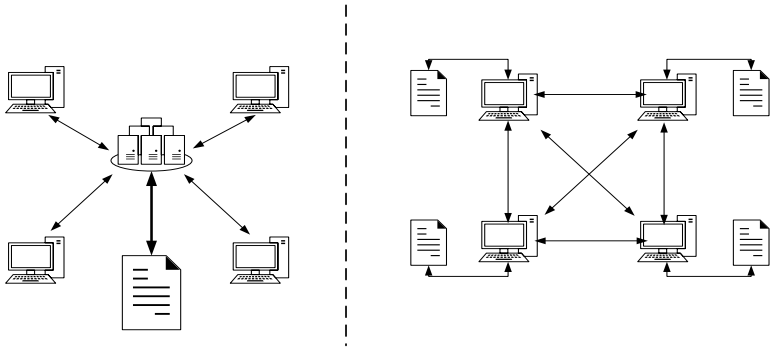

图 2.1 中心化记账方式和去中心化记账方式对比

Fig. 2.1 Centralized accounting Vs Decentralized accounting

区块链应用系统中的所有节点都保存完整的区块链数据，即每个节点在本地都有一条区块链，并不断的添加新的交易区块。区块链是由众多区块构成的，从创世区块开始一个区块一个区块的记录新的区块链数据。每一个区块都由区块头和区块体两部分组成。每个区块的区块头中都包含一个字段表示前一个区块的哈希值，区块自身的哈希值被后一个区块所包含。这样每一个区块都连接前一个区块和后一个区块，直到两端的创世区块和最新的区块形成了一条由区块组成的链，即区块链。

区块链的存储如图 2.2 如下所示。

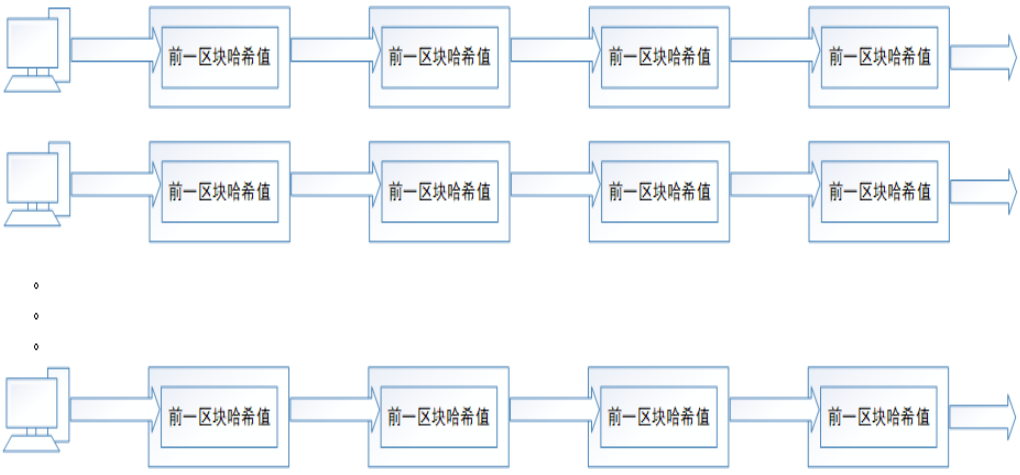

图 2.2 区块链的存储

Fig. 2.2 Blockchain storage

2.2.1 数据区块的基本结构

以比特币为例区块链的区块基本数据结构如表 2.1 所示。

(1) 神奇数：此字段长度固定为 4 个字节，内容固定为 0XD9B4BEF9,此字段用来作为区块之间的分隔符；

(2) 区块大小：此字段长度固定为 4 个字节，用于记录此字段之后的区块所有的内容的长度；

(3) 区块头：此字段长度固定为 80 个字节，包含区块头部的信息；

(4) 交易计数器：此字段长度可变（比特币为 1-9 字节，比特币交易数量限制即是 1M），用以记录区块中的交易数量并限制交易数量上限；

(5) 区块体：此字段长度可变，记录区块中所有包含的交易。

表 2.1 区块结构

Tab. 2.1 Block structure

大小	字段	描述
4 字节	神奇数	区块之间的分隔符
4 字节	区块长度	此字段之后的区块长度
80 字节	区块头	组成区块头部的字段
1-9（可变整数）	交易计数器	记录区块内的交易数量
可变大小	交易内容	记录区块内的交易数据

区块头部的数据结构如表 2.2 所示。

表 2.2 区块头部结构

Tab. 2.2 Block header structure

大小	字段	描述
4 字节	版本号	当前系统版本号
32 字节	前一区块哈希值	前一个区块哈希值
32 字节	梅克尔根	Merkle 树的根哈希值
4 字节	时间戳	区块的生成时间
4 字节	目标值	难度目标值

区块头部具体包含以下内容：版本号，长度固定为 4 个字节，用于表示当前系统的版本；前一区块哈希值，长度固定位 32 个字节；梅克尔 Merkle 根，长度固定为 32 个字节，梅克尔树的根节点，区块后面的所有交易会以树的形式两两进行哈希运算得到梅克尔树 [29]；时间戳，长度固定为 4 个字节，用以记录新的区块产生的时间；目标值 Target，长度固定为 4 个字节，目标值表示挖矿难度，目标值越大挖矿难度越低，区块所有内容最终哈希计算的结果小于目标值就满足条件产生新的区块；随机数 Nonce，长度固定为 4 个字节，每次哈希计算都变化直至计算出小于目标值，寻找随机数的过程就是挖矿的过程。

2.2.2 UTXO 模型

很多区块链系统中代币的存储及交易是以区块链地址中所拥有的未经花费的交易输出（Unspent Transaction Output，简称 UTXO）的形式存在的。在使用 UTXO 模型的区块链系统中只有地址的概念而没有账户，只有 UTXO 的概念没有余额的概念。UTXO 是区块链系统中不可分割的最小单位，是一个被区块链地址所有者锁定并记录于区块链上的表示一定数量代币的基本单位。每个 UTXO 上都记录着一定数量的代币，并且记录着其产生的交易的索引。通过 UTXO 的索引溯源，所有的 UTXO 都会指向一笔 Coinbase 交易。每个区块链地址拥有 0-N 个 UTXO，每个 UTXO 表示 0-N 个区块链代币。例如，比特币系统中比特币的最小表示单位称作“聪”，聪表示比特币系统及区块链技术的创始人中本聪，一比特币等于 1 亿聪比特币。

每个 UTXO 的最初来源都是 Coinbase 交易，即所有区块链代币都来自矿工产生新区块所奖励的代币，且所有 UTXO 都能根据自身的交易索引找到每个 UTXO 自其诞生以来的全部交易详情。交易的输入是 UTXO，交易的输出也是 UTXO，Coinbase 交易除外。交易的输入可以是来自一个 UTXO 也可以是来自多个 UTXO，输出同理。交易的余额将新的 UTXO 作为交易输出的一部分返还给原地址。实际交易中还会有一笔交易输出分给产生区块的矿工地址，称作交易费。

区块链应用系统中的每一个单笔交易中主要包含四个要素，即交易输入的 UTXO、交易的输入地址、交易输出的 UTXO 以及交易的输出地址。

区块链系统中具体的每一个单笔交易的输入与输出的 UTXO 详情如图 2.3 所示。

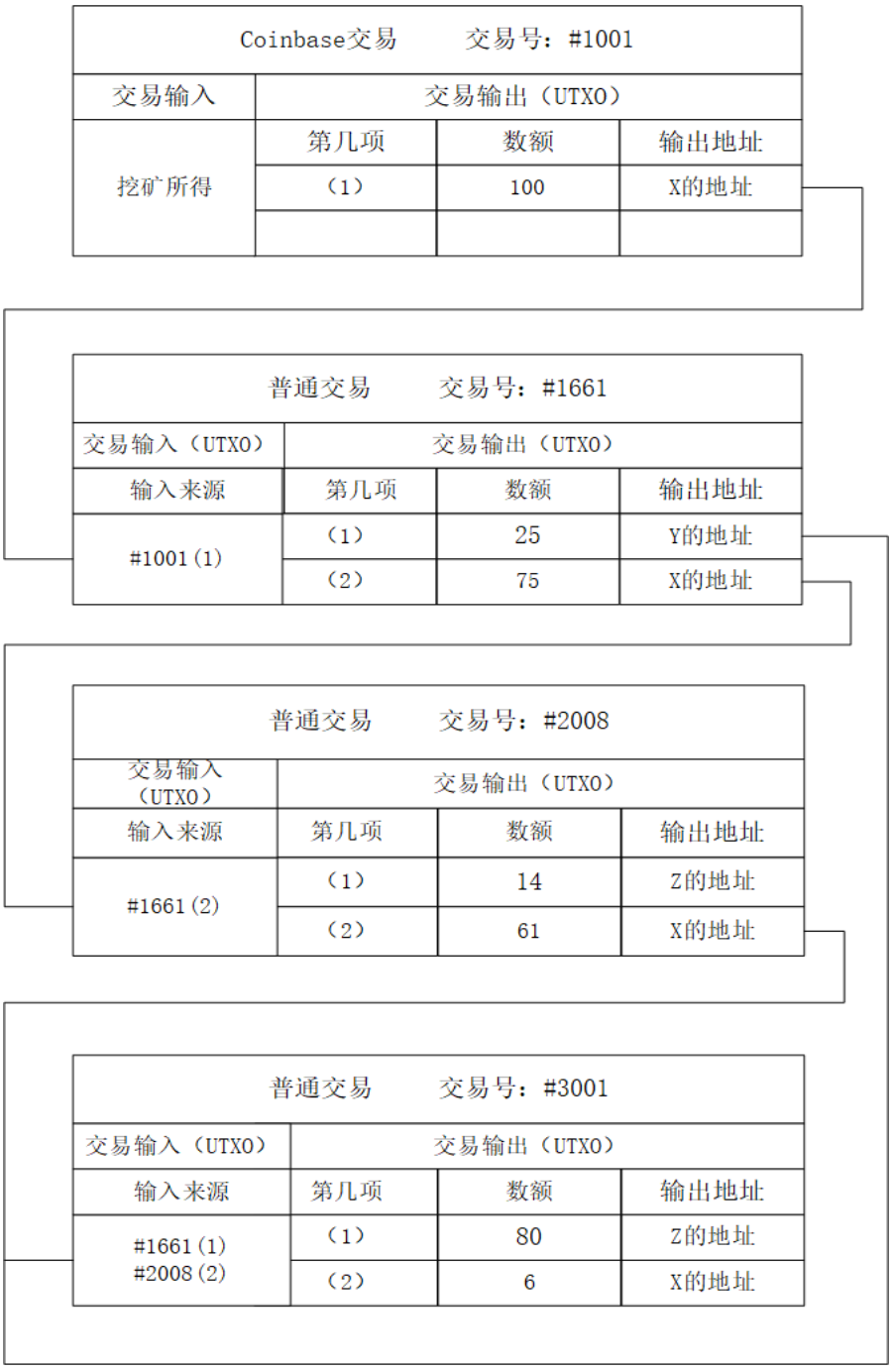

图 2.3 UTXO 交易输入与输出

Fig. 2.3 UTXO Transaction input and output

2.2.3 交易的基本结构

区块链数据区块中的交易内容主要分为两个部分，一部分记录了当前数据区块内所有交易记录总体情况，另一部分详细记录了每一笔交易的收支详情及梅克尔树节点值详情。

在每条交易记录的前面是所有交易的总体详情，主要包含以下子字段：版本号；交易输入数目；交易输入地址详情；交易输出数目；交易输出地址详情；交易时间戳。

交易记录是按每笔交易的输入与输出逐条列出的，每条交易记录的详情如表2.3所示。

表 2.3 交易记录结构

Tab. 2.3 Transaction record structure

大小	字段	描述
4 字节	版本号	当前系统的版本号
1-9 字节	输入数量	当前交易中包含的输入（UTXO）数量
32 字节	交易	指向交易包含的 UTXO 的哈希指针
4 字节	输出索引	被花费的 UTXO 的索引号，第一个是 0
1-9 字节	解锁脚本尺寸	用字节表示的后面的解锁脚本长度
可变长度	解锁脚本	一个达到 UTXO 锁定脚本中的条件的脚本
4 字节	序列号	目前未被使用的交易替换功能，设成 0xFFFFFFFF
1-9 字节	输出数量	当前交易中包含的输出（UTXO）数量
8 字节	总量	用聪表示的比特币值
1-9 字节	锁定脚本尺寸	用字节表示的后面的锁定脚本长度
可变长度	锁定脚本	一个定义了支付输出所需条件的脚本
4 字节	时间戳	一个 Unix 时间戳或区块高度号

2.3 区块链技术的基本原理

区块链其实是一个分布式的公共账本，包含所有发生在区块链应用系统上的交易。与传统的银行系统以及支付系统不同的是，区块链应用系统不再需要第三方

中央权威信任机构来做担保，只需要依靠区块链本身的去中心化去信任化机制就可以完成转账与交易的记录。

2.3.1 私钥公钥与地址

在区块链系统中交易需要靠区块链地址和该地址的公钥、私钥才能完成。接下来本文就以比特币为例介绍区块链地址、公钥、私钥已经它们之间的关系[30]。

私钥实际上就是一个随机生成的 256 位二进制数。在交易中私钥用于生成支付代币所必须的数字签名以证明对 UTXO 的所有权。从某种意义上讲，在区块链系统中私钥是一个代币地址上所有代币 UTXO 的所有权和控制权的唯一的也是最终凭证，一旦将私钥遗忘或者泄露，就等同于丢掉了代币或者是将代币拱手送人。

在区块链系统中私钥的生成也是有一定限制条件的。私钥需要是一个在 1 到 n-1 之间的任意一个 256 位二进制数，其中的 n 是由使用的椭圆曲线算法的阶所定义的。

私钥是一个区块链地址最终的、唯一的标识凭证，而区块链系统中的公钥就是由私钥生成的，区块链地址又是由公钥生成的。

公钥可以用私钥通过椭圆曲线算法计算得出。不过从私钥计算得出公钥的过程是单向的、不可逆的。由于椭圆曲线算法是单向运算[31]，逆运算是暴力运算的过程，因此我们可以轻易的通过私钥计算得出公钥，但却不能公钥计算出私钥。通过私钥计算得出公钥的计算公式为 K=k*G，其中 k 是私钥，K 所得到的公钥，G 是生成点的常数点。

由私钥生成公钥，由公钥生成比特币地址的过程如图 2.4 所示。

图 2.4 区块链地址生成

Fig. 2.4 Blockchain address generation

由公钥经过两次哈希计算并进行 Base58 编码的具体过程如图 2.5 所示。

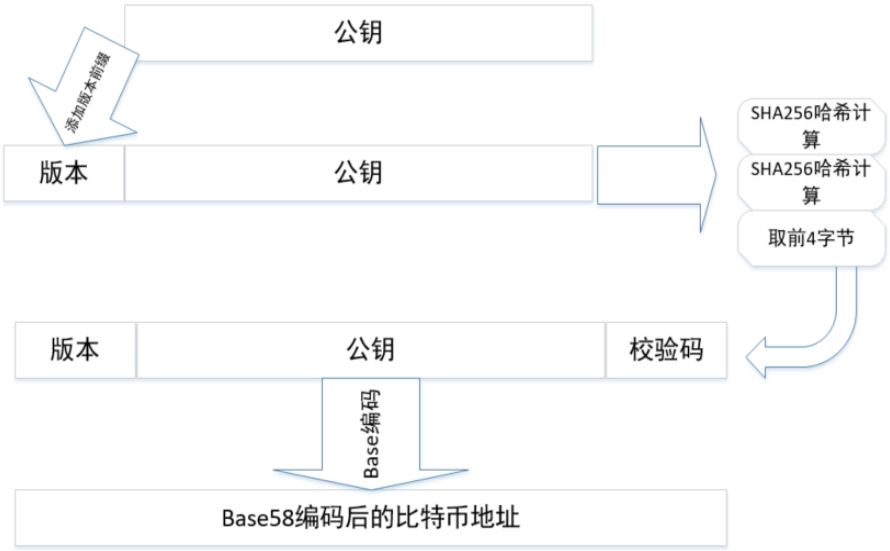

图 2.5 区块链地址编码

Fig. 2.5 Blockchain address code

区块链地址是一个由数字和字母组成的字符串，由公钥生成。首先在公钥前加上区块链系统的版本号，然后连续进行两次 SHA256 哈希运算后取前四个字节作为校验码加到公钥后面[32]。最后再用修改后的公钥进行 Base58 编码得到最终的地址。因为 Base58 的编码格式与十六进制格式转换结构位数不确定，所以最终得到的区块链地址位数也不是固定的。例如比特币的地址位数是 26 到 34 位之间不定，通常情况下比特币地址的位数多是 34 位。

哈希计算过程中改变一个字符或者一位数字都会使计算结果变得千差万别。

2.3.2 交易过程与脚本

那么私钥是如何在交易中证明自己对代币的所有权并允许代币进行交易的呢？其他节点又是如何验证输入的 UTXO 没有被花费的呢？答案是脚本和 UTXO 模型，区块链系统通过锁定脚本和解锁脚本来允许代币进行交易，通过 UTXO 模型来防止输入的代币是未被花费的，即双重支付或双花问题。

区块链技术中的脚本可以被理解为一种可编程的智能合约。由于区块链技术是去中心化的，那么所有节点就需要对所有的 UTXO、所有的交易行为都提前取得共识。这样以来，脚本技术的引入就显得至关重要了。脚本实际上就是一个集合了众多指令的列表。这些指令用于记录在交易过程中，交易输出地址如何获得这些输

出，以及花费掉自身收到的交易输出需要哪些附加的条件。通常情况下，交易输入方需要提供以下两个证据才能证明其的确拥有这些代币并允许该代币进行交易：第一个证据是公钥；第二个证据是签名，针对该交易的签名，证明代币的持有者拥有与上述公钥相对应的私钥。解锁脚本用 UTXO 的持有者发来的公钥和签名就可以解锁相应的代币 UTXO 从而使这些交易输入的 UTXO 被花费掉，使交易得到进行。然后锁定脚本再用交易输出方发来的公钥进行锁定，这样交易输出方就得到了属于他自己的 UTXO，交易得到完成。交易完成后就是广播交易，等待其他节点将交易打包到区块中，并保证区块被全网节点确认。上述过程就是共识过程，这也是本文研究的重点。防止双花问题主要是依靠 UTXO 模型实现的，只有 UTXO 才能作为输入进行交易。脚本还具有可扩展性、可编程性等。

2.4 共识机制

对全网的共识在分布式系统中是最核心的挑战之一[33]。对交易的共识、对区块的共识、对 UTXO 的共识也是区块链应用系统所需要解决的最核心的问题。因此，在区块链技术诞生以来的近十年之中，共识机制的发展是最迅猛的。

共识机制的过程简单来说就是决定哪个节点具有记录新账本的权利、决定哪个节点具有产生新的区块的权利、以及其他全网节点如何认同该节点记账和产生新的区块。脚本可以解决 UTXO 所属权、控制权以及交易的发行权的问题，UTXO 模型可以解决双重支付问题以及溯源问题，而全网对新的数据区块的共识问题就需要共识机制来解决了。

在现有的区块链应用系统中，公有区块链共识机制[34]主要分成两大类：一类是 POW（Proof of Work）工作量证明机制；另一类是 POS（Proof of Stake）权益证明机制[35]。其中 POS 权益证明机制之中的一个升级版本 DPOS 委任权益证明机制（Delegated Proof of Stake）也是一种比较流行的共识机制。

2.4.1 拜占庭将军问题

共识机制解决的问题实际上就是 P2P 网络中分布式总账的数据一致性问题。实际上共识机制解决的问题就是拜占庭将军问题（Byzantine Failures）。换句话说

拜占庭将军问题就是一个探讨怎样取得共识的问题。拜占庭将军问题最早是莱斯利-兰伯特（Leslie Lamport）于 1982 年提出的点对点通信中的基本问题[36]。

拜占庭将军问题的核心含义是指在存在着消息篡改以及消息丢失隐患的不可靠信道中，尝试依靠传递信息的方法实现信息的一致性是几乎难以成功的。因此，对信息一致性的研究时，通常假设信道是不存在问题的。

拜占庭将军问题所描述的是现实世界的信息与数据一致性问题的抽象化模型。在现实世界中，计算机和网络通信中会因为网络堵塞、单点故障以及黑客攻击等原因，而出现不可预知的问题 [37]。1980 年出版的 Marshall Pease 的论文中[38],首次提出了关于解决拜占庭将军问题的具体实施方案。自 Marshall Pease 的论文之后，众多关于拜占庭将军问题的解决方案与论文在会议以及期刊中提到。例如，著名的 Aardvark[39]以及拜占庭容错冗余(RBFT)[40]。

2.4.2 POW 工作量证明机制

POW 工作量证明机制首次见于比特币系统，比特币系统的共识机制也是 POW 工作量证明机制中的经典代表。POW 工作量证明机制主要核心思想就是全网节点通过大量的哈希运算去计算找到符合条件的区块哈希值，即找到使区块哈希值符合目标数 target 条件的随机数 nonce 来证明自己获取了新区快的铸造权。如果在一个新的区块尚未达成全网共识之时，就有许多节点同时计算出了符合条件的区块哈希值并产生新的区块广播，这样就会产生区块链的分叉。在分叉之后，其他节点会自动选择较长的链作为公链并在其上继续进行挖矿记账[41]。在若干个区块之后通过自然选择的结果，其他分叉的短链会被遗弃，最终只留有一条公链，比特币系统之中一般是 6 个区块之内解决分叉问题。人为依靠矿池算力会产生硬分叉，这时的新分叉是在原主链上产生的新的区块链 [42]。因此一般在比特币系统中交易确认需要等待 6 个区块，交易才算真正被全网节点所确认、交易才算真正的达到不可逆的状态[43]。POW 工作量证明机制的每一次共识过程都是全网节点同时参与的算力竞争过程[44]。

POW 工作量证明机制的主要挖矿以及共识过程如下。

（1）打包交易；

矿工节点接收 P2P 网络中的区块链交易信息并对交易进行验证。交易的 UTXO 输入方会提供针对该笔交易的数字签名和公钥、而交易的 UTXO 输出方则会提供公钥。矿工节点会根据 UTXO 输入方提供的公钥和签名生成对应的代币 UTXO 解锁脚本并对交易输入的 UTXO 进行验证。验证成功后，矿工节点用 UTXO 接收方提供的公钥信息生成锁定脚本并对之前解锁的 UTXO 进行锁定。

交易验证成功后，矿工节点将交易进行单向哈希运算作为新生成的梅克尔树的叶子节点。

交易打包成功后，矿工节点将该交易信息存于交易池中。

（2）打包区块；

矿工节点将所有接收到的区块链交易打包后，将生成的梅克尔树叶子节点两两进行哈希计算生成新的梅克尔树节点，生成的节点继续两两进行哈希计算，最终得到梅克尔树的根节点。整个梅克尔树就是区块链交易的一个交易树，由于哈希计算的特性，每一笔交易只要改动一点点所有的相关梅克尔树节点以及根节点的哈希计算结果都会变得天差地别。因此，区块链的区块可以防止篡改交易数据。

矿工节点计算出梅克尔树的根节点后，将该根节点与前一区块的哈希计算值、版本号、目标数、时间戳和随机数等区块头信息一起打包进行哈希计算。

（3）寻找幸运数；

矿工节点对区块头信息进行多次哈希计算，每次的随机数都变化，直到所得到的区块哈希值满足条件就可以生成新的区块了。区块哈希值满足的条件是区块哈希值前 N 位为 0，即区块哈希值小于目标数。满足区块哈希值的那个随机数即是所寻找的幸运数，POW 工作量证明机制挖矿的实质就是寻找幸运数的过程。

（4）广播区块；

矿工节点在生产新的区块后，将所找到的区块信息广播给 P2P 网络中的其他矿工节点。

（5）区块共识。

在所有矿工节点挖矿的过程中，可能会有多个不同的新区块被生成。整个区块链系统在无中心节点的情况下，抉择出其中的一个区块所在的链作为主链，其他区

块所延伸出的链为侧链。这个去中心化的、去信任化的抉择过程就是区块链技术共识的过程，这个过程的运行机制与准则就是区块链技术的共识机制。

POW 工作量证明机制的优点是安全、可靠、运行稳定等，缺点是消耗大量的算力与电力、区块产生时间长、确认等待时间长、易受到矿池的绑架产生分叉等等。

2.4.3 POS 权益证明机制

POS 权益证明机制首次见于 2012 年出现的点点币系统。在点点币系统的共识机制中首次引入了币龄的概念[45]，后在黑币系统中省去了币龄的概念改为币权的概念。POS 权益证明机制的核心思想有两点：一点是节点获取区块的铸造权的概率与节点所拥有的可用权益成正比关系；另一点是区块链应用系统产生新的代币的方式，从 POW 工作量证明机制中的产生区块的固定奖励，更改为节点在产生区块时清空币龄获得利息，即新的区块链代币。

币龄的概念就是区块链地址所拥有的币值与持有的时间的乘积，POS 权益证明机制在清空币龄时按币龄产生利息，即新的区块链代币。

POS 权益证明机制的优点是减少了大量的算力与电力消耗、缩短了区块产生时间以及区块确认时间等，缺点是安全性与可靠性降低、更容易分叉等等。

2.4.4 其他流行的共识机制

DPOS[46]委任权益证明机制是 POS 权益证明机制的一种升级版本，也是一种比较流行的共识机制。DPOS 委任权益证明机制的核心思想是拥有权益的节点可以像股份公司的股东一样将自己的权益委任给信任的、可靠的代理人，这些代理人拥有权益后可以获得产生新的区块的权利，如果代理人不正常产生区块则罢免并重新选举代理人。

此外，其他主要的流行的共识机制还有 PBFT[47]（Practical Byzantine Fault Tolerance）拜占庭容错算法、以太坊的 Casper 抵押权益共识机制以及量子链的 MPOS 互惠权益证明机制等。

第 3 章 对现有区块链共识机制方案的问题分析

自区块链技术问世以来，矿池集中化的问题一直是制约区块链技术发展的主要问题。矿池集中化的出现违背了中本聪创建区块链技术的初衷，违背了去中心化。

3.1 POW 中的矿池集中化问题

POW 工作量证明机制自从问世以来，一方面其安全、可靠以及去中心化的特性受到了学术界和商业界的热捧，而另一方面其容易导致矿池集中化[48]、消耗大量算力与电力、区块生成时间与区块确认时间漫长的缺点也为学术界以及商业界所诟病。

图 3.1 显示的是自 2017 年 11 月 6 日至 12 月 6 日一个月时间内比特币系统的全网平均算力分布情况。

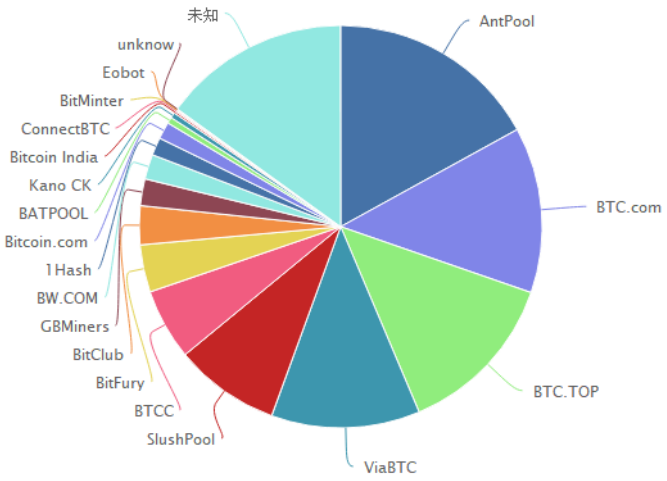

图 3.1 比特币算力分布

Fig. 3.1 Bitcoin computing power distribution

从图 3.1 可以看出，共有四家矿池的算力超过了 10%的全网算力，这四家矿池分别是 AntPool（17%）、BTC.com（13.32%）、BTC.TOP（13.32%）以及 VIABTC（11.93）。四大矿池总计占了全网算力的 55.57%，如果算上其他的小矿池的的话，所有矿池总记占了全网算力的 85%。这是一串非常可怕的数字，我们知道从理论上讲，超过 51%全网算力就可以发动“女巫攻击”[49]，即有能力摧毁比特币的生

态网络。如果这些矿池联合在一起后果是不堪想象的，这严重违背区块链技术去中心化的特性、也严重违背了区块链技术的初衷。

事实上近半年来炒的非常火热的比特币分叉事件，就是矿池算力集中化的一个“苦果”。分叉的初衷其实也是善意的、具有美好愿景的。由于最初自身数据结构的设定只能容纳 1M 大小的交易。在系统运行的早期由于交易量比较小，这个交易容量还是很充足的。但是随着区块链技术的日益火爆，1M 大小的区块容量越来越显得捉襟见肘，严重时会发生交易积压的情况，极端情况有交易被压了近半个月的时间。因此，最初为了解决区块容量大小的问题，各大矿池联合推出了 BCH 比特币现金(BitCoin Cash 原简称 BCC)，区块大小为 8M。自从推出 BCH 比特币现金之后，各大矿池又联合推出了比特币黄金 BTG Bitcoin Gold。BTG 提出的目标就是解决矿池算力集中化的问题，将比特币系统的挖矿算法从 SHA256 算法改为 Equihash 算法，以抵制挖矿性能强大的专业矿机 ASIC 矿机，从而达到真正的去中心化。然而事实并非如此，矿池算力的本质并没有发生变化，矿池组织依然可以通过聚集大量的专业显卡矿机以达到算力垄断的目的。从 ASIC 矿机挖矿到显卡矿机挖矿并没有本质的变化，只是将算力的量级降低了，矿池组织依然横行，因此 BTG 的出现并没有真正解决矿池集中化的问题。反而，这种由矿池组织支持进行 IFO（Initial Fork Offerings）的行为，更加佐证了矿池算力集中化对区块链技术的严重危害。

3.1.1 矿池算力集中化的原因

导致矿池算力集中化的原因主要有两个，一是矿池利用庞大的资金以及现金的计算设备堆积算力达到垄断效果；二是普通矿工节点因为算力过低取得区块铸造权的概率非常小，因而加入矿池组织，将自己的算力贡献给矿池，帮助完成矿池分配的计算任务。当矿池挖到代币时，按算力比例分配给矿工一点点代币。

实际上这两个造成矿池算力集中化的原因是相互促进且恶性循环的关系[50]。最初因为矿池组织堆积了庞大的算力，从而导致全网平均总算力大幅度上升。因此普通矿工节点的算力占全网算力比例大幅度下降、获得区块铸造权的概率降低、取得的比特币收益降低，从而导致其在利益的驱动下加入了矿池组织以维持收益。这

样由于众多普通矿工节点的算力的加入，矿池组织所掌控的算力比例继续上升，矿池收益更多。矿池收益更多之后继续矿大算力规模，从而导致全网总算力继续上升，其他未加入矿池的普通节点的收益继续降低，并在利益的驱动下加入了矿池。最终造成了全网算力被若干个矿池组织瓜分的局面。全网走向了中心化的歧途。

由于 POW 工作量证明机制是靠算力来维持区块链的安全性、可靠性以及一致性的，几乎所有 POW 工作量证明机制都没有提出对矿池算力集中化的解决方案。而少数比较著名的针对矿池问题的 POW 工作量证明机制也都没有妥善解决此问题。例如，比特币的分叉区块链应用系统 BTG 虽然抵制了 ASCI 矿机挖矿避免了算力向天文数字的方向发展，但本质问题并没有解决，依然会造成矿池算力的集中化。实质上 POW 共识机制只靠算力计算的机制是导致矿池集中化的最根本原因。

3.2 POS 中的矿池集中化问题

POS 权益证明机制为了解决矿池算力集中化的问题而走向了另一个极端，抛弃了以算力来维持安全性、可靠性以及一致性的方法。POS 权益证明机制的核心是引入了币龄和币的概念，来将繁琐的、大量的、无用的哈希计算彻底抛弃。POS 权益证明机制的安全性、可靠性和一致性不再依赖于算力，其共识过程也几乎不耗费算力，只需要少量的哈希计算。因此，POS 权益证明机制彻底解决了算力集中化的问题，但却又带来了权益集中化的新问题。从算力集中化到权益集中化，只是区块铸造权垄断的形式发生了变化，其本质并没有改变，仍然会造成中心化的后果。

点点币是第一个使用 POS 权益证明机制的区块链应用系统。点点币的出现就是为了解决矿池算力集中化和消耗大量算力的问题 。但是点点币没有预想到去除了算力影响的 POS 权益证明机制反而更加容易分叉。因为现在只要聚集大量的币龄就可以掌控区块的铸造权，连购置算力设备都省掉了。点点币之后的黑币、未来币都是在点点币的共识机制基础上改进，这几种共识机制大体相似，也都没有解决矿池的问题。

POS 权益证明机制去除算力因素引入币龄的概念依然避免不了矿池集中化的问题。虽然 POS 权益证明机制在性能和消耗上大大减少，但是由于缺少了工作量证明，在安全性、可靠性略有降低。

3.3 POW+POS 混合证明机制

由于 POW 工作量证明机制和 POS 权益证明机制自身的设计缺陷都不能妥善的解决区块链技术矿池集中化的问题。因此很多研究人员就考虑到是否能够将二者结合起来，取长补短利用各自的优势设计一种 POW+POS 的混合共识机制。

目前还没有一种成熟的 POW+POS 的混合共识机制应用于区块链系统中，多数都只是处于概念阶段。一般来说 POW 和 POS 混合共识机制的想法的主要分为四类：第一类是区块链应用系统初期应用 POW 工作量证明机制，达到一定的区块高度后系统切换到 POS 权益证明机制。这种共识机制实质上就是 POS 权益证明机制，并没有什么改变；第二类是 POW 和 POS 证明机制在区块链系统中轮流切换使用，这种共识机制目前只是概念并没有实际的区块链应用系统；第三类是以太坊的 Casper 投注权益证明机制。Casper 投注权益证明机制的核心思想是节点在确认新产生的区块时将自身的一定权益也投注在这个新区快上，本质上是将权益作为另外一种形式的工作量进行消耗。但是 Casper 投注共识机制截止至目前也还只是概念，尚未应用到实际的区块链系统之中。第四类是量子链的 MPOS 互惠共识机制等混合共识机制。这些共识机制多处于概念阶段或应用初期，尚未经过实践验证或公布技术原理。

虽然 POW+POS 的混合共识机制目前处于概念阶段，没有接受实践的检验，但是 POW 和 POS 混合的共识机制这个大方向是没错的。最新的一些区块链应用系统的共识机制也主要以 POW+POS 的混合共识机制为主。

本文第 4 章设计的基于权益调节的工作量证明机制即是一种混合 POW 和 POS 的共识机制。本文在 POW 工作量证明机制中引入 POS 权益证明机制中的币龄的概念用于调节哈希计算的目标数，从而调节不同矿工节点的挖矿难度，以达到减弱矿池集中化的目的。

第 4 章 POWS 共识机制方案设计

区块链应用系统运行的安全性以及可靠性是需要其底层区块链技术提供支持与保障的[51]。而作为区块链技术的核心技术，共识机制就是为区块链系统的运行提供支持与保障的关键所在。POW 与 POS 混合的共识机制已经被看作是区块链技术共识机制未来的发展方向与主流。

本文秉承着 POW+POS 混合的思想，引入 POS 共识机制中的权益（币龄）概念用于调节 POW 共识机制的挖矿模式，设计了一种基于权益调节的工作量证明机制 POWS。本章将从总体设计架构、节点网络、共识机制与挖矿算法、基本数据结果等方面详细介绍 POWS 的设计与实现。

4.1 POWS 共识机制总体架构设计

如图 4.1 所示，本文设计的 POWS 共识机制系统由应用层、扩展层、共识层和存储层四部分组成。

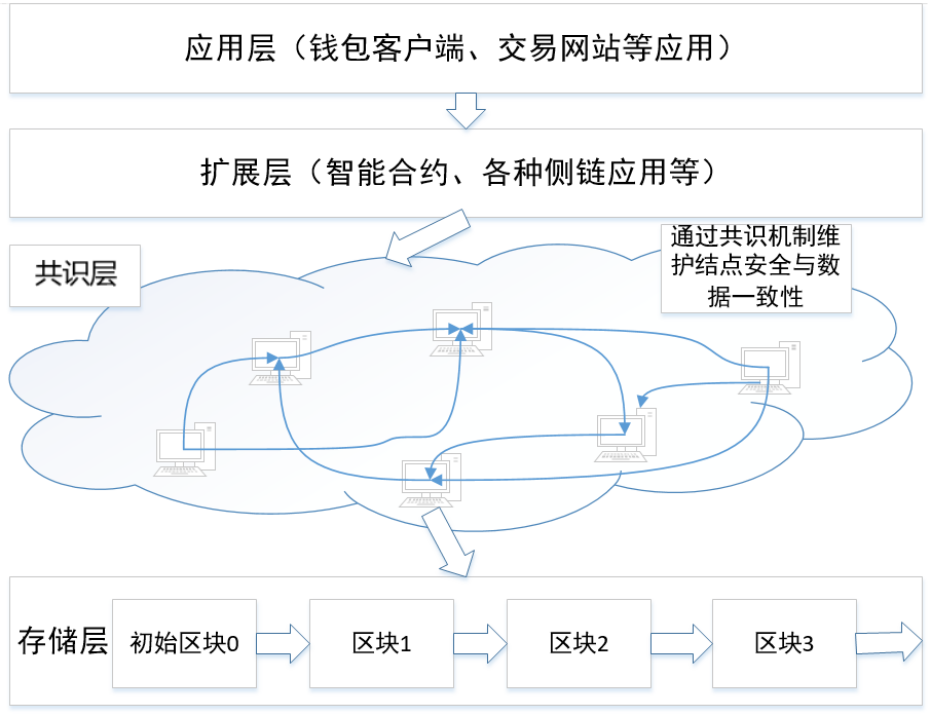

图 4.1 系统架构

Fig. 4.1 System structure

应用层的功能是为用户提供具体的区块链接口，满足用户的具体需求。最有代表性的应用包括钱包客户端、交易平台、通讯软件等。

扩展层的功能是引入智能合约、闪电网络等侧链应用。

共识层是本文所研究的核心内容。如图 4.2 所示，共识层通过共识机制实现所有节点的本地区块链数据的一致性。共识层通过共识机制、挖矿算法和区块链版本协议等维护区块链应用系统运行的安全性和可靠性。本文共识层所采用的共识机制就是 POWS 共识机制。

图 4.2 共识层

Fig. 4.2 Consensus layer

存储层的功能是存储完整的区块链数据。区块链系统中所有节点都存储完整的区块链数据，以保障系统的安全性和可靠性。每一个矿工节点在本地存储的区块链数据的基础上挖矿，同时接收自来自整个系统的交易信息和区块同步信息，通过共识层的共识机制来维护系统的数据一致性、安全性以及可靠性。

4.2 底层节点 P2P 网络

区块链技术是以 P2P 网络作为应用基础的，所有的公有区块链应用系统都是建立在 P2P 网络基础之上的。区块链技术的去中心化特性与共识机制也都是针对

P2P 网络而言的、也都是在 P2P 网络的基础实现的。搭建一个区块链应用系统的前提就是搭建一个相适应的 P2P 网络。

所有的节点在所搭建的 P2P 网络之中，都是完全平等的、没有任何中心节点、完全去中心化。

4.2.1 节点设置与初始化

整个区块链网络中的所有节点地位完全平等，节点存储完整地区块链数据。节点接收交易信息、区块同步信息、进行挖矿、并在共识机制的作用下达成全网共识。

每当有新的节点加入区块链网络时，节点首先要进行区块同步。节点向网络中的其他节点发起区块链同步请求，同步最新的区块链主链数据并进行挖矿。区块链系统会为所有的节点（包括需要初始化的新节点）提供搜索当前 P2P 网络中的挖矿节点（即活跃节点）的功能，从而记录相应的节点 IP 地址并进行区块信息同步。因此，当有新节点加入到系统之后，系统会向区块链网络发起活跃节点 IP 请求。系统中的其他节点接收到请求后会根据自身存储的信息返回活跃节点的 IP 地址列表。节点根据网络中的其他节点返回的活跃节点 IP 地址列表，向其中的活跃节点发送区块信息同步请求。

4.2.2 节点间通信

在新加入系统的节点发送区块同步请求通信之前，还需要与相对应的节点先建立通信连接。

节点之间建立连接时，发送请求的节点首先将自身的系统版本信息（包括节点自身的时间戳、节点自身的系统版本号、节点自身存储区块链系统主链区块高度等信息）发送给对应的节点，以请求建立节点间的通信连接。对应的节点在收到发送的系统版本信息之后，会同样的把自身的系统版本信息返回到新加入的节点，以回应对方的建立通信连接的请求。建立通信连接的双方节点，会对双方的系统时间戳进行确认，如果双方节点的系统时间戳一致则相互返回请求确认信息并成功建立通信连接。如果双方的系统时间戳不一致，则不能建立通信连接。

通信双方节点在建立连接之后就可以进行区块同步请求了。双方节点之间的通信连接每半个小时就会向对应的的节点发送连接维护信息 Keepalive。Keepalive

信息用于向对应的节点发送信息告知对方通信连接依然正常存在。节点每半个小时发送 Keepalive 信息，这半个小时就被称作保活周期。节点在通信时，如果三个保活周期时间内都未接收到对应节点发送的 Keepalive 信息，就会自动断开通信连接。

4.2.3 区块信息同步

新加入系统的节点与其他节点保持通信连接后就可以进行区块信息同步了。新加入系统的节点最初都会在本地存储创世区块，然后向其他节点发送区块信息同步请求。新加入系统的节点进行区块信息同步的这个过程被称作新区块的初始化。当新的节点同步完区块信息，再本地存储完整地区块链主链才能被称为全节点。

在系统中只有全节点才能参与挖矿，参与区块链系统的维护。如果节点不作为全节点存在，不同步区块信息、不在本地存储完整的主链信息，就只能利用区块来应用系统进行转账、交易、查询等相关拓展应用。轻节点只是在使用区块链系统，而不是参与维护区块链系统。

4.3 POWS 基于权益调节的工作量证明机制

4.3.1 POWS 去中心化共识过程

中本聪发明的共识机制是一种去中心化条件下自发运作的机制[52]。这种自发的特性体现在没有经过明确选举或者在不能达成共识的时间内，完成异步共识，即区块链系统中的每一个独立的节点在既定好的程序规则下异步交互自发形成共识。

本文所设计的共识机制应是由每个独立的节点经过四种独立过程相互作用而形成的：

（1）每一个独立全节点按照既定的规则与标准对每一笔数字交易独立检验；

（2）节点将通过 POWS 共识机制检验的交易记录独立打包到新生成的区块内；

（3）每个节点独立的对新生成的区块进行验证，验证成功后连接到其本地存储的区块链数据中；

（4）每一个节点接收到交易记录或者区块同步信息时，如果发现存在着多条区块分叉链的情况，需要独立地按照 POWS 共识机制对所有的区块分叉链进行独

立的选择，本文设计的 POWS 共识机制的规则是选择出工作量最大的区块分叉链作为主链，即选择最长的一条区块分叉链作为主链。

本文设计的 POWS 共识机制以及挖矿流程如图 4.3 所示。

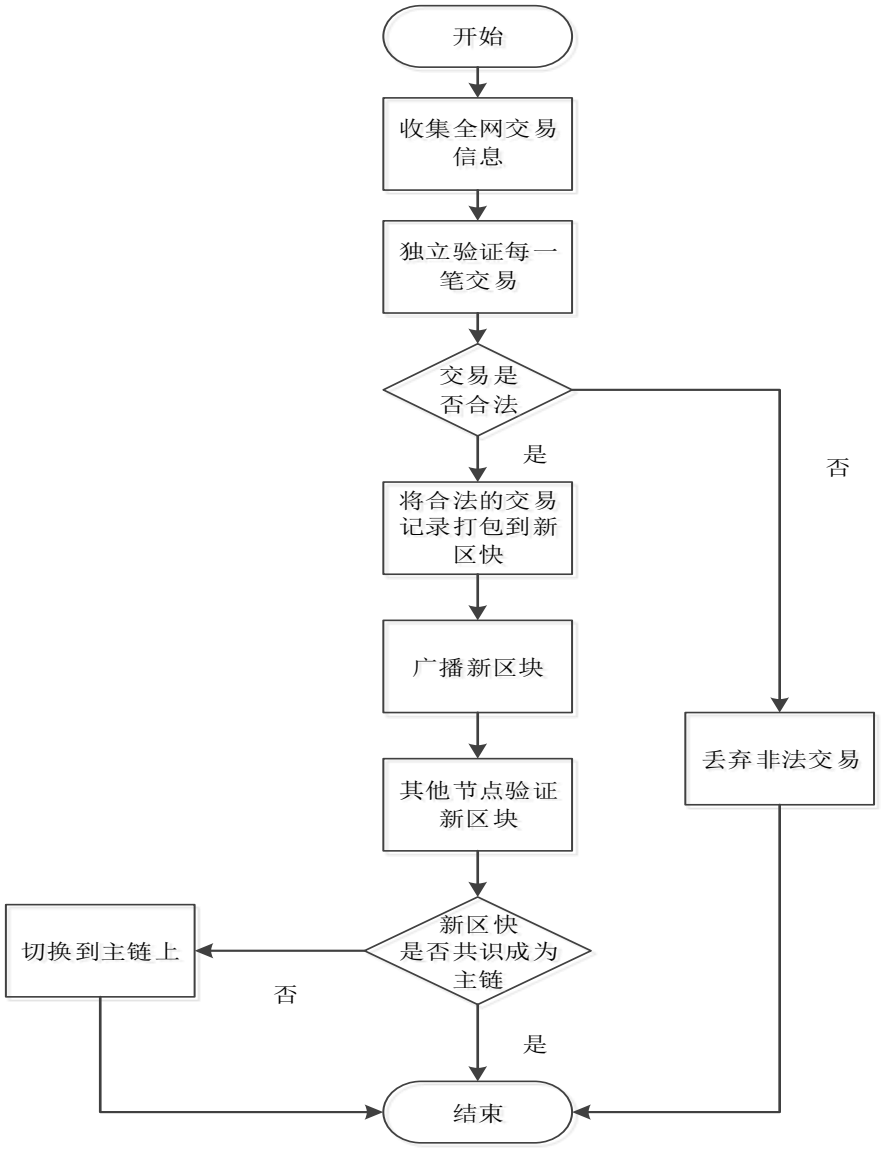

图 4.3 POWS 共识过程

Fig. 4.3 POWS Consensus process

每一个独立的节点的这四种独立的过程相互作用并最终达成整个区块链网络的自发性共识。这四种独立的过程使任意节点组合出区块链自己的权威、可信、公开的总账。

因此，POWS 共识机制的本质就是每个矿工节点都按照上述的四种独立过程，接收来自区块链应用系统中的每一笔交易记录、验证每一笔交易记录、打包所有交易记录到区块内、生成新的区块、验证新生成的区块、按规则选择分叉链并最终达成共识，存储相同的区块链数据。

4.3.2 POWS 交易的独立校验

区块链应用系统的钱包（客户端）会收集交易输入 UTXO、提供正确无误的 UTXO 解锁脚本、创建用于交易输出方接收的 UTXO 输出等一系列操作构建交易信息。随后钱包会将交易记录广播发送到区块链应用系统中的其他节点，使得交易在区块链网络中传播并被收入到矿工节点的交易池中。

每一个矿工节点在接收到区块链交易记录后，需要对交易进行独立地验证。每一个矿工节点只有在验证交易记录合法有效之后才后把交易记录打包到新区块之中，才会把交易记录发送给区块链网络中的其它节点。

每个节点在独立地验证每笔交易的时候都需要遵照以下标准。

(1) 交易记录的数据结构和语法必须正确；

(2) 交易的输入以及输出列表均不能为空；

(3) 交易记录的大小需要小于 MAX_BLOCK_SIZE 字段的值；

(4) 每笔交易的 UTXO 总量必须符合规定范围；

(5) 如果交易输入的 UTXO 总量小于输出的 UTXO 总量，则废弃交易；

(6) 每一个输入的 UTXO 解锁脚本必须按照该 UTXO 的锁定脚本来验证；

(7) 每一个输入的 UTXO 必须是合法的、可用的；

(8) 交易记录中的签名数量必须小于签名操作的数量上限；

(9) 交易输入的 UTXO 的哈希值不能等于-1、0，Coinbase 交易不能被中继；

(10) 如果交易输入的 UTXO 已经存在于交易池中的其他交易记录的输入之中，则废弃该交易；

(11) 一笔交易的交易费不能过低以至于不能够被打包到新的区块之中；

(12) 交易记录中所有输入的 UTXO 以及输出的 UTXO 的值应当符合规定的范围，即大于零，小于 2100 万；

(13) nLockTime 字段必须小于或等于 INT_MAX 字段的；

(14) 区块主链中或交易池中的已验证交易必须是存在的；

(15) 每一个输入的 UTXO，需要在交易池以及区块主链上验证到该 UTXO 的输出交易记录，否则该交易是为一个孤立的交易并添加到孤立交易池之中；

(16) 如果一个交易的输入的 UTXO 中包含由 Coinbase 交易输出的 UTXO，则该输入的 UTXO 至少需要等待 COINBASE_MATURITY 字段 100 个确认；

(17) 解锁脚本只能将数字压入栈中；

(18) 锁定脚本需要符合 isStandard 字段的格式，此字段格式用于拒绝非标准交易。

矿工节点在接收到交易记录后，会按照上述的标准独立的对交易信息进行检验。检验成功后，矿工节点将交易继续向全网广播并依据接收的顺序将通过独立验证的交易加入到交易池中。

4.3.3 POWS 交易的独立打包

矿工节点将所有通过验证的交易记录保存在本地的交易池中。交易池，也被称作内存池，是用来存储已经被矿工节点验证合法，但尚未被添加到区块中的交易记录。矿工节点一边继续收集、验证以及中继交易记录，一边将交易池中的交易记录打包添加到候选区块之中。候选区块就是在包含足够的工作量之前的区块，即尚未找到符合区块哈希规则的区块。当区块包含了足够的工作量证明（即通过数学计算得到了符合规则的区块哈希值），候选区块就能成为真正的区块广播到整个区块链网络。

矿工节点在将交易池内的交易记录打包到候选区块时会有一个优先级顺序。这个优先级顺序并不是按照交易的矿工费决定的，而是按照 UTXO 的币龄决定的。

单个 UTXO 的币龄的计算公式如公式 4.1 所示。

$$CoinAge=Value*InputAge \tag{4.1}$$

其中 Value 表示 UTXO 具有的代币值，InputAge 表示 UTXO 的存在时间。一个交易记录中所输入的所有 UTXO 的币龄和越大，该交易记录在交易池中的优

先级就越大。交易优先级是输入的所有 UTXO 的币龄与交易总长度相除得到的，具体的计算公式如公式 4.2 所示。

$$Priority=\sum_{i=0}^{n} CoinAge_i/TransactionSize \quad (4.2)$$

其中 TransactionSize 表示交易的总长度。交易输入的 UTXO 值得单位是聪、年龄的单位是区块数、币龄的单位是字节、交易记录的单位是字节。交易优先级大于 115200000 的交易具有较高的优先级，1152000 是一个币值的 UTXO 经历了一天的区块数（约 288 个区块），交易长度为 256 字节所计算得出的优先级。

区块中用于记录交易的前 50 字节按照优先级排序分配给具有较高优先级的交易记录，无论该交易记录所包含的矿工费有多少。剩余的字节按交易费的高低分配，区块长度的上限为 MAX_BLOCK_SIZE 字段所记录的值。

4.3.4 POWS 的币创交易

矿工节点在将交易池中的交易记录打包到候选区块之前，必须创建一个币创交易（即 Coinbase 交易）打包到候选区块之中。几乎所有的区块链应用系统都包含 Coinbase 交易，其目的主要是为了给予矿工节点奖励以及增发区块链数字货币。而本文所设计的 POWS 权益调节工作量证明机制，则对 Coinbase 交易的功能进行了增加，增加了清空币龄的功能。

这里清空的币龄与前一小节的单个 UTXO 的币龄不同，这里清空的是矿工节点的区块链地址上所拥有的全部 UTXO 的币龄总和。该总币龄和地计算公式如公式 4.3 所示。

$$SumCoinAge=\sum_{i=0}^{n} (Value_i*Input_i) \quad (4.3)$$

Coinbase 交易总是处于所有交易中的第一条。其他的区块链应用系统的 Coinbase 交易都不包含输入的 UTXO 和其解锁脚本，只包含输出的 UTXO 和锁定脚本。POWS 的 Coinbase 交易则与此不同，即包含输入的 UTXO 也包含输出的 UTXO、即包含解锁脚本也包含锁定脚本。

POWS 的 Coinbase 交易的输入 UTXO 就是矿工节点自身所拥有的全部 UTXO，输出的 UTXO 只有一个且接收地址仍为矿工节点本身的地址。Coinbase 交易输出的 UTXO 的值是输入的 UTXO 值的总和、区块内所有其他交易的交易费总和、区块矿工奖励三项的和，POWS 暂设定奖励为 1。

POWS 的 Coinbase 交易的作用有三个：清空了矿工节点用于参与挖矿的总币龄和；将区块内的交易费收入支付给矿工节点；将生成区块的奖励支付给矿工节点。

4.3.5 POWS 区块的生成与挖矿算法

区块主要分为区块头和区块体两个部分，区块体主要记录的就是交易记录。区块体中主要记录了的综合则包含了输入输出交易详情、Coinbase 交易记录及梅克尔树节点详情、每一笔交易记录详情及梅克尔树节点详情。

梅克尔树在区块链系统中主要用来记录每一笔交易的详情。包括 Coinbase 交易在内，所有的交易记录都需要进行哈希计算。所有交易记录摘要的哈希计算结果值作为梅克尔树的叶子节点。梅克尔树的叶子节点的数目必须是偶数，如果候选区块内的交易的数目是奇数，则需要复制最后一笔交易记录凑成偶数。

这些作为梅克尔树的叶子节点的交易记录两两的、逐层的相互组合进行哈希计算形成新的上层梅克尔树节点，并最终得到梅克尔树的根节点。梅克尔树的根节点将所有的交易记录哈希计算成了一个 32 字节长的哈希值。区块内的任意一笔交易记录只要更改一个符号，最终的梅克尔树的根节点哈希值都会变得天差地别。梅克尔树的根节点作为记录交易记录摘要的字段存在于区块头之内。

矿工节点生成区块头之和需要将分割字段、区块长度、区块头、权益记录、交易计数器以及交易记录详情一起打包生成候选区块。

生成候选区块之后，矿工节点需要尝试计算不同的随机数 Nonce，以找到合适的随机数 Nonce 使得计算出的区块哈希值符合规则，即区块哈希值小于目标难度值。

挖矿的过程就是矿工节点不断尝试不同的 Nonce 进行哈希计算的过程。POWS 基于权益调节的工作量证明机制也需要大量的哈希计算，即工作量来证明

区块的铸造权。POWS 共识机制生成区块并进行哈希计算找到符合条件的区块哈希值的具体过程如算法 1 所示。

Algorithm 1: Proof of Work Based on Adjusted Stake (POWS)

```
POWS(header, SumCoinAge):
max-nonce ← 2 ^ 32   // 随机数上限，约为 40 亿
target ← coefficient*2^(8*(exponent-3))*(SumCoinAge)^(1/2)
    //POWS 共识机制难度目标值计算公式
for  nonce ←0  to  in max-nonce
    do  hash-result ← hashlib.sha256(str(header)+str(nonce)).hexdigest()
        //计算候选区块哈希值
        if  long(hash_result,16) < target:
        return  (hash-result , nonce)
        //验证候选区块哈希值是否小于难度目标值，小于则返回 hash-result 以及随机数 nonce
return  (‘’ , nonce)
    //未找到符合条件的候选区块，则返回最终随机数 nonce，此时 nonce 即为随机数上限 max-nonce
```

计算统计哈希计算速率的过程如算法 2 所示。

Algorithm 2: Calculate the hash rate

```
Calculate-hash-rate (hash-result, SumCoinAge)
Start-time ← time.time()
New-block ← ’test block with transactions’ + hash-result
  //新区块的区块头必须包含前一个区块的哈希值
(hash-result, nonce) = POWS(new-block , SumCoinAge)
//找到新区块的随机数 nonce
End-time ← time.time()
eta ← end-time - start-time
if eta > 0
  do  hash-rate=float(long(nonce)/eta)    //计算哈希速率
      return hash -rate
return  false
```

矿工节点获取收益的效率取决于矿工挖矿的效率，即节点进行哈希计算的平均速率。而矿工节点进行哈希计算的平均速率主要与两个因素相关：第一个因素是计算机或是矿机的硬件条件；第二个因素是挖矿的难度。

计算机或是矿机的硬件条件的最直接反映就是算力。算力越大挖矿的收益就越，在不考虑算力成本的情况下。

挖矿算力属于外界因素且算力集中化的问题正是 POWS 共识机制要解决的问题。而第二个因素挖矿难度就是指区块头中的难度目标值字段。难度目标值 Target 越大，挖矿难度就越小。因此，POWS 共识机制可以通过调节难度目标值 Target 来调节挖矿难度，从而抵制算力与币龄集中化的问题。POWS 共识机制在难度目标值 Target 的计算公式中引入了矿工节点的总币龄和的概念用于调节 Target。

难度目标值 Target 的计算公式如公式 4.4 所示。

$$\text{Target} = \sqrt{\text{SumCoinAge}} * \text{cofficient} * 2^{(8*(\text{exponent}-3))} \quad (4.4)$$

公式 4.4 中的参数 SumCoinAge 就是矿工节点的地址上所有的 UTXO 的币龄之和，该参数是用于调节挖矿难度的；参数 Exponent 和参数 Coefficient 表示挖矿难度，这两个参数的初始值时根据比特币网络在区块高度为 49500 时的取值。在区块头中有一个字段是难度目标，这个难度目标不是难度目标值 Target，而是一个 8 位的十六进制数。这个 8 位的十六进制数的前两位即是公式 4.4 中的 Coefficient，后六位是公式 4.4 中的 Exponent，这两个参数用于周期性调节整个区块链系统的难度从而使出块时间稳定。这两个参数 Cofficient 和 Exponent 对于所有矿工节点都是相同的。而参数 SumCoinAge 是针对每一个矿工节点而言的，每个矿工节点的总 UTXO 币龄和都会不同。因此拥有的 SumCoinAge 不同，矿工节点的挖矿难度就不同。

POWS 共识机制挖矿的效率受算力和权益两个因素的影响。挖矿矿池需要的成本也由单一的算力或者权益变成了两者皆需要。

4.3.6 POWS 区块的独立验证

当矿工节点找到符合条件的区块哈希值之后，该候选区块就可以作为新生成的区块在 POWS 共识机制应用的区块链网络中广播了。当区块链网络中的其它在节点接收到该新区块的广播信息之后，节点必须对该新区块进行独立的合法性验证。

节点对新区块的验证主要包括以下几项：对区块中所有交易记录的合法性验证，具体验证流程以及验证标准与矿工节点在打包交易时对交易记录的验证相同；对矿工节点的 Coinbase 交易的验证，验证 Coinbase 交易输入与输出的 UTXO 的合法性；对难度目标值 Target 的验证，验证难度目标值的正确性以及 SumCoinAge 的正确性；对区块哈希值的验证，验证区块哈希值是否合法；对区块时间戳得验证，验证区块时间戳与前面的区块是否矛盾；对梅克树根节点的验证，验证交易记录是否被修改；验证其它区块头部各字段是发合法；对新区块语法以及数据结构得合法性进行验证。

每个节点在接收到新区块的广播信息之后，必须按照以下验证标准进行独立的新区块验证：

(1) 新区块的各项语法以及数据结构必须合法；

(2) 各项交易记录均需按照前面章节 4.3.2 中的交易的独立验证标准，进行合法性验证；

(3) 交易记录中的一笔交易必须是 Coinbase 交易，且必须对 Coinbase 交易的合法性进行验证；

(4) 新区块的大小必须在规定范围之内；

(5) 新区块的哈希值必须合法，即新区块哈希值小于区块难度目标值 Target；

(6) 新区块的难度目标值 Target 必须合法；

(7) 新区块的矿工节点输入 UTXO 总币龄和 SumCoinAge 必须合法；

(8) 新区块的时间戳的时间必须在其前一区块时间戳的时间之后。

节点在对新区块的合法性进行独立的验证并通过之后，就会将该区块作为暂时的区块链主链存储在本地的区块链副本之中。在节点未接收到其他节点广播的

不同新区块广播信息的情况下，节点在这个区块后继续添加了 12 个区块之后，就可以基本认为该区块及其前面的区块成为了主链。

4.3.7 POWS 区块的本地存储与独立选择

节点在对新区块进行独立的验证并通过之后，需要将该新区块连接到其父区块之后，即区块头中前一区块哈希值所指向的区块后。此时节点在寻找新区块父区块之时，会发现新区块可能不仅仅是主链上最新的一个区块一种可能。新区块及其父区块可能出现的位置有以下几种可能。

(1) 父区块为主链上的最新一个区块且待确认区块范围内无分叉，新区块成为暂时的主链最新区块。此时，节点只需正常将该新区块添加到其父区块之后并继续中继该新区块的广播信息即可；

(2) 父区块非主链上的最新一个区块但位于主链上的待确认区块范围内，此时若新区块所在分叉上工作量更大，即分叉链的区块数目更多，则视该新区块为暂时的主链并将挖矿工作和交易池更新到该主链之上。若新区块所在分叉上工作量更小，即分叉链的区块数目更少，则将新区块连接到父区块之后但不切换主链。若新区块所在分叉的工作量与暂时的主链相等，则比较二个分叉链上的所有区块权益之和，即矿工 Coinbase 交易输入的 UTXO 总币龄和，哪个分叉权益更大则作为暂时的主链存在。若新区块成为了暂时的主链，则继续中继其广播信息，否则继续在原暂时的主链上挖矿；

(3) 父区块不位于主链上的待确认区块范围之内，则废弃该新区块；

(4) 找不到对应哈希值的父区块，则废弃该新区块。

事实上在区块链网络中连续几个区块都产生分叉概率非常的小、几乎不可能发生，因此区块链分叉总会在几个区块之内就解决掉分叉问题并迅速形成整个区块链网络的共识、形成一条主链。POWS 共识机制为了更稳妥一些，将确认区块的数量定为了 12 个区块。区块链分叉示意图如图 4.5 所示。

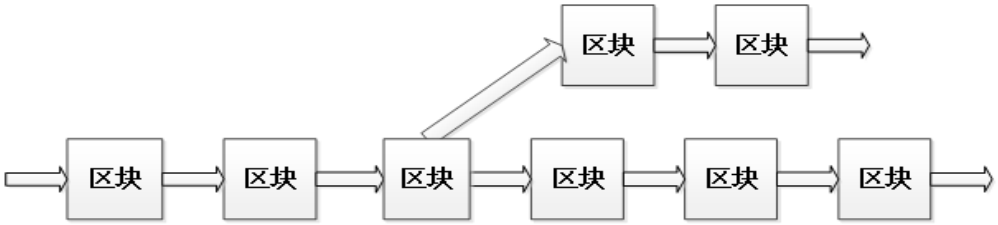

图 4.5 区块链分叉

Fig. 4.5 Blockchain bifurcation

新区块在经过了 12 个区块后被整个区块链网络认定为主链后就可以确定位于主链上了。

第 5 章 POWS 模型系统的实验及结果分析

本文在实验室环境下，对第四章提出的 POWS 共识机制进行了基本性能和抗矿池化两个方面的实验，并对实验结果与 POW 共识机制和 POS 共识机制进行了对比分析。

5.1 实验环境介绍

5.1.1 硬件介绍

本文所进行的实验均是在实验室的服务器上构建 P2P 网络、模拟区块链公有链网络实现的。实验在实验室的 1-8 号服务器上进行测试实验。

实验室的 1-8 号服务器的具体硬件配置情况如表 5.1 所示。

表 5.1 实验硬件环境说明

Tab. 5.1 Experiment hardware environment description

名称	内存	内核数	硬盘	系统	内网 IP
服务器 1 号	16GB	4	500G	Ubuntu 16.04	192.168.10.1
服务器 2 号	16GB	4	500G	Ubuntu 16.04	192.168.10.2
服务器 3 号	16GB	4	500G	Ubuntu 16.04	192.168.10.3
服务器 4 号	16GB	4	1T	Ubuntu 16.04	192.168.10.4
服务器 5 号	16GB	4	1T	Ubuntu 16.04	192.168.10.5
服务器 6 号	16GB	4	500G	Ubuntu 16.04	192.168.10.6
服务器 7 号	16GB	4	300G	Ubuntu 16.04	192.168.10.7
服务器 8 号	16GB	4	500G	Ubuntu 16.04	192.168.10.8

5.1.2 软件介绍

本文实验所使用到的几个主要软件的版本信息如下：Bitcoin Core 版本为 v14.02；PeerCoin 版本为 v0.6.1；Qt Creator 版本为 3.1.0；Berkeley DB 版本为 6.4.9。最重要的比特币核心 Bitcoin Core 的版本信息如图 5.1 所示。

图 5.1 Bitcoin Core 版本信息

Fig. 5.1 Version information of the Bitcoin Core

5.1.3 实验数据集

本文中抗负载实验使用的数据集是比特币系统的交易数据。比特币交易数据可以通过任意一个比特币全节点获取。本文实验选取了比特币系统自创世区块到第 495000 区块的所有交易数据，并对交易数据稍作规范化处理以适应其他两个区块链共识机制的交易结构。比特币系统的部分交易数据集如图 5.2 所示。

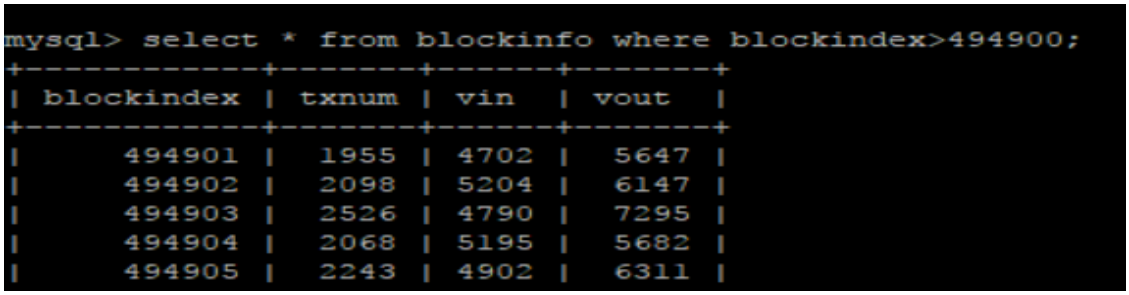

图 5.2 Bitcoin 交易数据集信息

Fig. 5.2 Bitcoin Transaction data set

5.2 实验方案

本文进行了基本性能和抗矿池化两个方面总计 5 个实验。

基本性能实验。

（1）平均出块时间对比实验；

（2）抗负载对比实验。

抗矿池化实验。

（1）平均出块效率随算力变化对比实验；

（2）平均出块效率随币龄变化对比实验；

（3）POWS 矿池对非矿池节点利益驱动实验。

5.2.1 实验基本设置

本文在实验室的 8 台服务器上总共开了 100 个性能配置相同的虚拟机模拟区块链测试网络中的矿工节点。每个虚拟机启动都安装配置测试实验所需的环境。本文实验使用比特币系统作为 POW 共识机制，使用点点币系统作为 POS 共识机制。每个虚拟机都作为一个矿工节点存在，整个实验中共有 100 个这样的矿工节点。实验使用的网络环境是在实验室内部搭建的 P2P 测试网络，每个矿工节点在初始条件下分配一万个代币进行平均出块时间实验，后续实验根据实验需求调整所有矿工节点的初始代币数目。

5.2.2 平均出块时间对比实验

本文设计的 POWS 共识机制在进行抗矿池集中化效果的实验之前，需要对其基本性能进行测试。

所有的矿工节点依次连续运行 POWS 共识机制、POW 共识机制和 POS 共识机制。每种共识机制连续运行 10 天，三种共识机制总计运行 30 天。在进行每次测试开始之前，将每种共识机制的每个节点初始代币均分配相同初始代币数目和硬件设置。统计每种共识机制的区块高度并计算出平均出块时间。

5.2.3 抗负载对比实验

将比特币的交易数据集针对 POS 共识机制和 POWS 共识机制进行规范化处理。分别在三个区块链共识机制上并发 500000 条、1000000 条、2000000 条、3000000 条、5000000 条、10000000 条交易，统计它们完全处理所有交易需要的区块数目并计算三种共识机制的平均每个区块处理交易数量。

5.2.4 平均出块效率随算力变化对比实验

由于 POS 共识机制的挖矿几乎不耗费算力，而且算力对其出块效率也没有影响，本文实验只对 POWS 和 POW 两种共识机制进行测试实验。

在两种区块链共识机制运行时分别对其中的十各单独的矿工节点持续增大其算力，即通过改变虚拟机配置或在服务器上添加高性能显卡实现算力的增加。本文实验为两个共识机制的每个实验节点分配的算力从 10Mhash/s、30Mhash/s、50Mhash/s、70Mhash/s、90Mhash/s 到 110Mhash/s 逐渐增加并使系测试统连续运行十天。运行结束后统计两种共识机制中，节点在算力增加的情况下平均出块效率的变化情况。根据统计的实验结果分析比较两种共识机制下，节点的平均出块效率随着算力增加的变化情况。

5.2.5 平均出块效率随币龄变化对比实验

由于 POW 共识机制没有用到币龄、币、权益等概念且币龄对 POW 挖矿也每有任何影响，本文实验挖只对 POWS 和 POS 两种共识机制进行测试实验。

在两种区块链共识机制运行时分别对其中的十各单独的矿工节点持续增大其算力，即通过改变为每个实验节点分配的初始代币数目实现币龄的增加。本文实验为两个共识机制的每个实验节点分配的初始代币数目从 10Mhash/s、30Mhash/s、50Mhash/s、70Mhash/s、90Mhash/s 到 110Mhash/s 逐渐增加并使系测试统连续运行十天。运行结束后统计节点在不同权益（币龄）情况下出块的效率。根据统计的实验结果分析比较两种共识机制下节点与出块效率（收益）随着权益（币龄）变化情况。

5.2.6 矿池对非矿池节点利益驱动对比实验

本文实验将整个区块链测试网络中的 10 个节点联合起来组成矿池与非矿池节点的出块效率进行对比实验测试。

在 POWS 共识机制中，本文实验为矿池节点依次分配全网 5%、10%、15%、20%、25%、30%、35%、40%的算力和初始代币进行矿池实验。在 POW 共识机制中，本文实验为矿池节点依次分配全网 5%、10%、15%、20%、25%、30%、35%、40%的算力进行矿池实验。在 POS 共识机制中，本文实验为矿池节点依次分配全

网 5%、10%、15%、20%、25%、30%、35%、40%的初始代币进行矿池实验。三个共识机制依次运行 14 天，每一种矿池运行 2 天。运行结束后统计节点在三种共识机制的不同矿池分配比例情况下矿池节点与非矿池节点的平均出块效率。根据矿池节点和非矿池节点的平均出块效率计算出每种共识机制的矿池节点与非矿池节点出块效率比。根据统计的实验结果分析比较三种共识机制下矿池节点与非矿池节点出块效率比，即矿池对非矿池节点的利益驱动。

5.3 实验结果与分析

5.3.1 平均出块时间对比实验

三种共识机制的平均出块时间如图 5.3 所示。

POW 共识机制的平均出块时间最长，且远长于另外两个共识机制； POWS 共识机制平均出块时间居中； POS 共识机制的平均出块时间最短；三个区块链的平均出块时间均相对稳定。

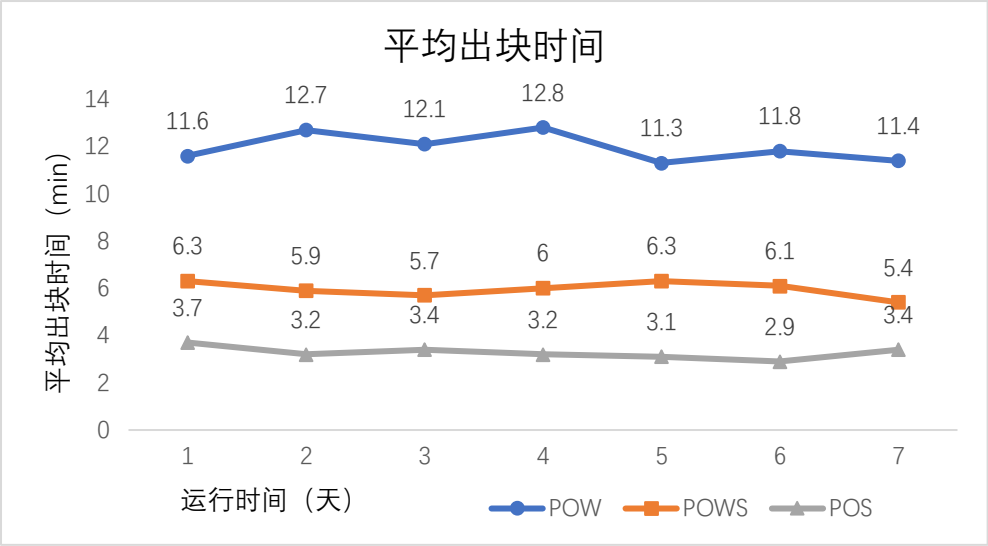

图 5.3 平均出块时间

Fig. 5.3 Average time of make block

POW 共识机制自身具有难度周期性调节机制，每隔 2016 个区块对难度系数进行调节，以使系统的平均出块时间稳定在 10min 左右。本实验中的 POW 共识机制的平均出块时间略高于 10min 应该是实验环境下算力规模与节点规模过小的原因造成的。POW 共识机制的平均出块时间最长且远长于两外两种共识机制的原因

是 POW 共识机制需要大量的哈希计算但却又没有任何降低目标难度（10min）的设置。POWS 共识机制去除了 POW 共识机制中 10min 难度目标的设置。POWS 共识机制中挖矿难度系数 Cofficient 和 Exponent 固定且设置为开始平均出块时间实验前 POW 共识机制的即时难度系数值。POWS 共识机制比 POW 共识机制多了根据每个节点币龄进行挖矿难度降低的设置，应用 POWS 共识机制的区块链共识机制的平均出块时间远低于 POW 共识机制。POS 共识机制几乎不需要挖矿，这就省去了大部分进行哈希计算的时间，POS 共识机制的平均出块时间也最短。三个区块链共识机制都是运行在性能稳定、无变化的 P2P 网络之上，所以平均出块时间均无剧烈变化。

5.3.2 抗负载对比实验

如图 5.4 所示在大量交易并发条件下，POWS 共识机制的区块处理交易能力是最强的。POW 共识机制和 POS 共识机制在大量交易并发条件下的区块处理交易能力大致相当。三种区块链共识机制的交易处理能力都是随着交易并发量的增大而降低的。

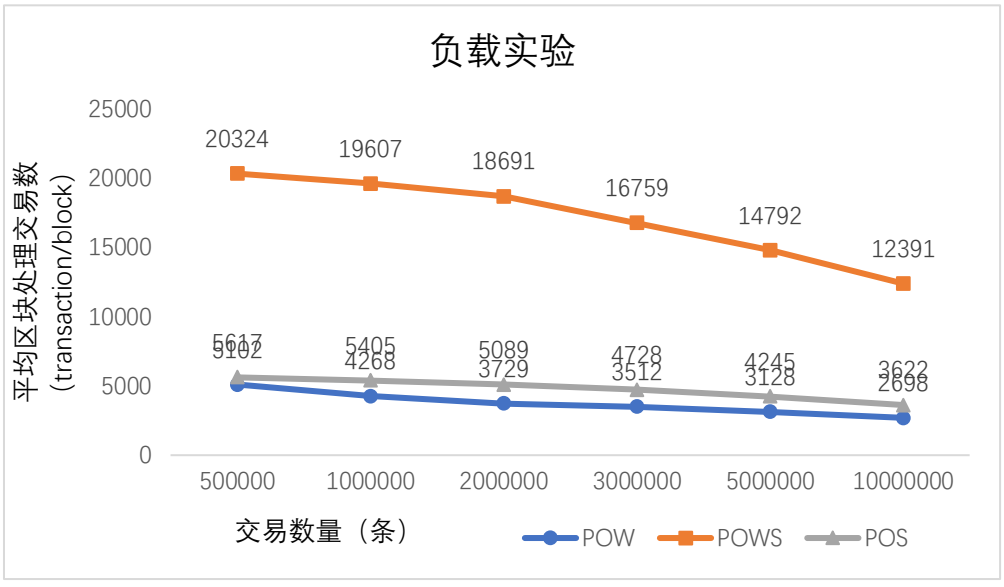

图 5.4 负载实验

Fig. 5.4 Load experiment

POW 共识机制和 POS 共识机制对区块容量都有大小限制。POW 共识机制的区块大小限制是 1M，POWS 共识机制将这个大小限制更改为 4M，因此 POWS 共识机制的交易处理能力才更强。随着交易并发量的增大，三种区块链共识机制的处理交易的能力都会因交易拥堵而降低。

5.3.3 平均出块效率随算力变化对比实验

如图 5.5 所示，本文所设计的 POWS 共识机制的出块效率随算力的增加而增加的更少，受算力的影响要小于 POW 共识机制。造成这种现象的原因是 POWS 共识机制比 POW 共识机制多了币龄的条件难度目标值。

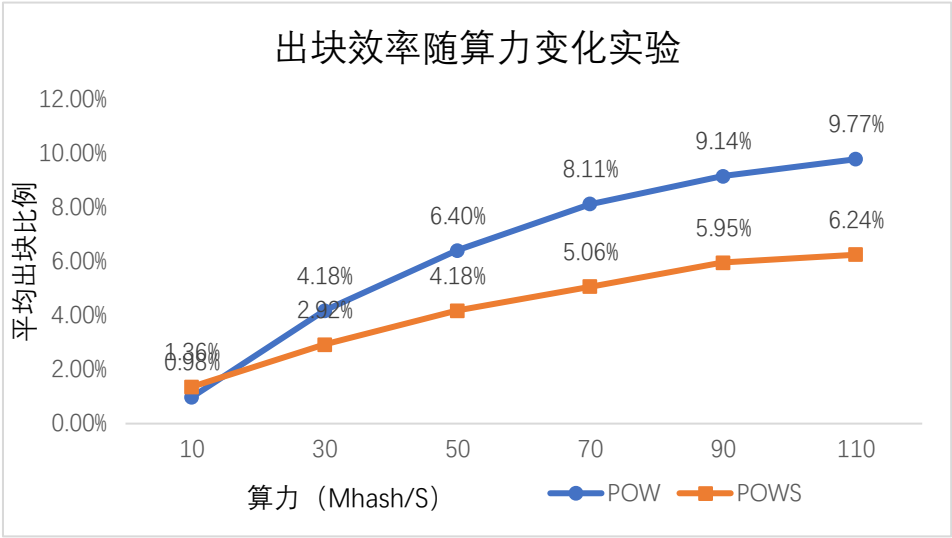

图 5.5 出块效率与算力实验

Fig. 5.5 Block efficiency and calculation of power experiment

5.3.4 平均出块效率随币龄变化对比实验

如图 5.6 所示，本文所设计的 POWS 共识机制的出块效率随币龄的增加而增加的更少，受币龄的影响要小于 POS 共识机制。造成这种现象的原因是 POWS 共识机制比 POS 共识机制多了算力这个影响因素。POWS 依然需要工作量证明，就必然受到算力的影响。

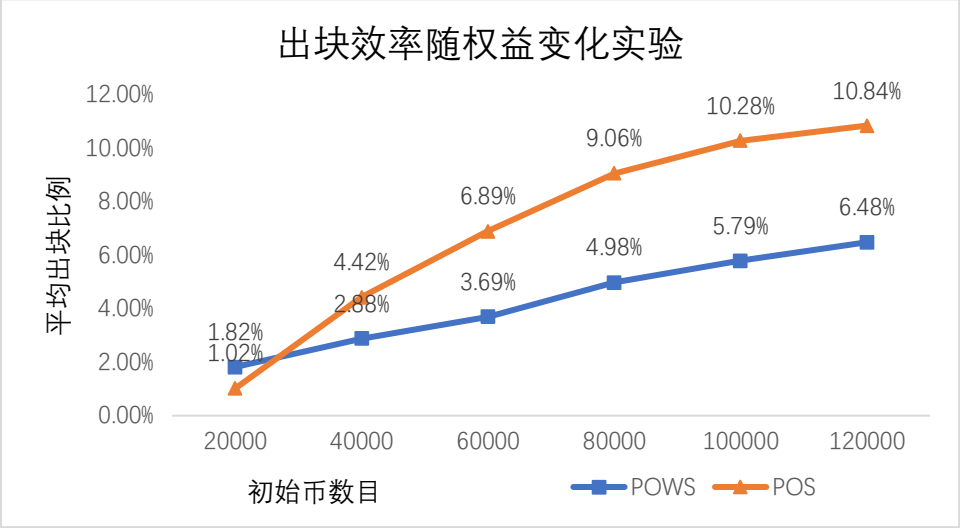

图 5.6 出块效率与权益实验

Fig. 5.6 Block efficiency and stake experiment

5. 3. 5 矿池对非矿池节点利益驱动对比实验

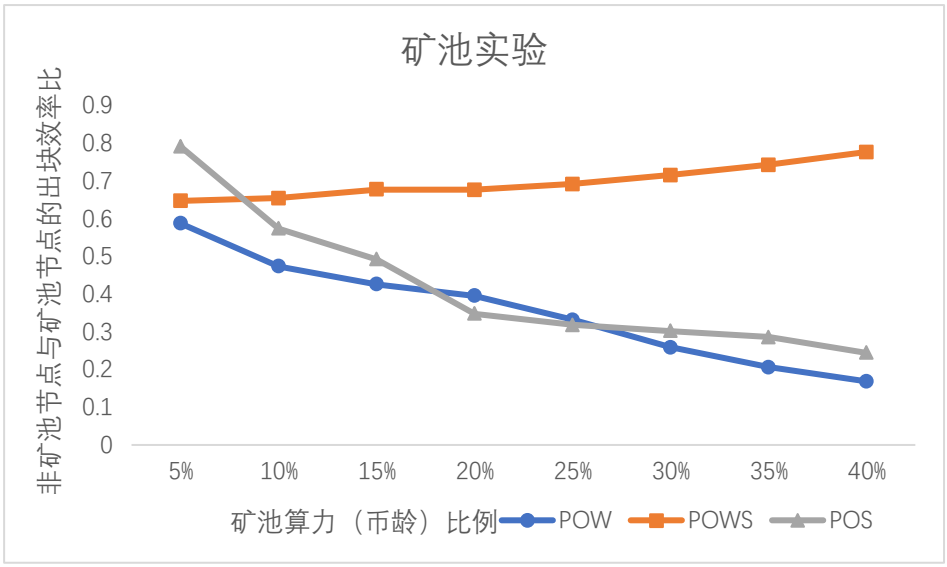

图 5. 7 POWS 矿池实验

Fig. 5.7 POWS Mine pool experiment

如图 5.7 所示，本文所设计的 POWS 共识机制中，非矿工节点与矿工节点的平均出块效率比例最高，且比例最高接近 0.8 左右。POW 共识机制和 POS 共识机制的非矿工节点与矿工节点的平均出块效率比例，在矿池算力或币龄较小时同样比较高，但是随着矿池算力或币龄币龄越来越大时变得越来越小。这种情况

下，非矿池节点和矿池节点的收益差距巨大，矿池对非矿池节点的利益驱动也是巨大的。造成这种现象的原因是 POWS 共识机制中新的挖矿算法对高算力和高币龄进行了制约。算力和币龄变得越大，挖矿难度降低的就越少。

从实验结果及分析可以看出，虽然随着算力和币龄的增加挖矿难度降低的越来越少，但是矿池节点的挖矿难度依然一直是低于非矿池节点的。POWS 共识机制降低了矿池节点与非矿池节点的平均出块效率差距，但仍有差距。事实上这些差距并不会全部兑现且矿池节点相比于非矿池节点有着很多弊端。

在现实中矿池还会对矿池节点收取费用，这样在 POWS 共识机制中真实的矿池节点与非矿池节点的出块效率比应跟高一些。

而区块链技术的宗旨是去中心化，矿池的集中化挖矿模式是受到很多矿工排斥的。而矿池中心化的挖矿模式还会带来很多新的问题。

（1）矿池中心化挖矿详情不可信

加入矿池的矿工节点并不会知晓矿池究竟生成了多少区块、自身贡献的算力和币龄占矿池的总比例、自身是否找到了随机数等。这一切都是靠矿池自己公布的，但是矿池给出的信息未必是可信的，这正是区块链技术所要解决的不可信问题。

矿池节点依据中心化的矿池提供的不可信信息获取收益这本身就是不合理的、存在风险的。

（2）矿池中心化管理代币不可信

矿工节点加入矿池需要将自身的代币通过智能合约的形式转给矿池。而转给矿池的代币是否被用于挖矿，矿工节点是不知道的。矿池的中心化模式管理代币是不可信的。

POWS 共识机制中矿池节点与非矿池节点的平均出块效率比差距较小、矿池收取费用、节点加入矿池有诸多弊端，因此在 POWS 共识机制较好地减弱了矿池对非矿池节点的利益驱动。

第 6 章 总结与展望

6.1 总结

区块链最重要的特点就是去中心化，而这个特点现在正面临着前所未有的威胁。在区块链公有链应用系统中广泛存在着矿池组织，囤积大量的算力和币龄，吸引普通矿工节点加入矿池以达到垄断区块铸造权的目的。矿池集中化破坏区块链技术公平、公正、去中心化的初衷。针对此问题，本文设计了一种基于权益调节的工作量证明机制，POWS 共识机制，以达到抗矿池集中化的目的。

POWS 共识机制在 POW 工作量证明机制的基础上，引入了 UTXO 总币龄和的概念，用于调节难度目标值 Target。POWS 针对不同矿工节点所拥有的不同 UTXO 总币龄和，分配不同的挖矿难度。POWS 通过挖矿算法调节挖矿难度，使算力和币龄增长越大时挖矿难度降低的越少。POWS 通过权益和算力两个因素共同调节挖矿难度，摆脱节点对算力或是币龄的单一因素过度依赖。

本文针对提出的 POWS 共识机制，从基本性能和抵御矿池效果两个方面进行了实验，得出以下结论：

（1）与 POW 共识机制和 POS 共识机制相比，POWS 共识机制中非矿池节点与矿池节点的平均出块效率比更高，矿池对非矿池节点的利益驱动更小。

（2）POWS 共识机制的平均出块效率，随算力或币龄的增长而增长的速度趋缓。

上述结论证明，本文提出的 POWS 共识机制合理可行，该机制能够达到对矿池集中化有效抑制的目的。

6.2 展望

在今后的工作中，还需要对以下论文内容做进一步的研究。

（1）POWS 共识机制仍需进行大量的哈希计算，消耗大量的算力，在日后的工作中需进一步研究降低 POWS 共识机制的算力消耗；

（2）POWS 共识机制的平均出块时间仍然慢于 POS 共识机制，在日后的工作中需进一步研究缩短 POWS 区块的生成时间。

参 考 文 献

[1] Xu X, Pautasso C, Zhu L, et al. The Blockchain as a Software Connector[C]. Software Architecture. IEEE,2016:182-191.

[2] Pilkington M. Blockchain Technology: Principles and Applications[J]. Social Science Electronic Publishing,2016.

[3] Sixt E. Ethereum[J].2017.

[4] Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]. Security and Privacy. IEEE,2016:839-858.

[5] Nakamoto S.A peer-to-peer electronic cash system[J]. Journal for General Philosophy of Science,2008.39(1):53-67.1

[6] Ametrano F M. Bitcoin, Blockchain and Distributed Ledger Technology[J]. Social Science Electronic Publishing,2016.

[7] Böhme R, Christin N, Edelman B, et al. Bitcoin: Economics Technology and Governance[J]. Journal of Economic Perspectives,2015,29(2):213-238.

[8] Schrijvers O, Bonneau J, Dan B, et al. Incentive Compatibility of Bitcoin Mining Pool Reward Functions[J].2016.

[9] Xia Q, Zhang F J, Zuo C. Review for Consensus Mechanism of Cryptocurrency System[J]. Computer Systems & Applications,2017.

[10] Aste T. The Fair Cost of Bitcoin Proof of Work[J]. Social Science Electronic Publishing,2016.

[11] Spasovski J, Eklund P. Proof of Stake Blockchain: Performance and Scalability for Groupware Communications[C]. The, International Conference on Management of Digital Ecosystems.2017.

[12] Saeki M. Elliptic Curve Cryptosystems[J]. Mathematics of Computation, 1997, 2(4):1024-1028.

[13] 李实.挖矿背后的秘密 SHA-256 加密算法浅析[J].微型计算机,2014(10):117-121.

[14] Dahlberg R, Pulls T, Peeters R. Efficient Sparse Merkle Trees[M]. Secure IT Systems. Springer International Publishing, 2016.

[15] 詹克团.矿池中挖虚拟数字币的方法和装置.CN 104915249 A[P].2015.

[16] Zohar A. Bitcoin[J]. Communications of the Acm, 2015, 58(9):104-113.

[17] 曾建伟.一种包含智能合约的区块链网式数据库及工作方法. Block chain intensive database and working method comprising intelligent contracts: CN 107103098 A[P].2017.

[18] Swan M. Blockchain: Blueprint for a New Economy[M]. O'Reilly Media, Inc.2015.

[19] Alstyne M V. Why Bitcoin has value[J]. Communications of the Acm, 2014, 57(5):30-32.

[20] Zohar A. Bitcoin: under the hood[J]. Communications of the Acm, 2015, 58(9):104-113.

[21] Sikorski J J, Haughton J, Kraft M. Blockchain technology in the chemical industry: Machine-to-machine electricity market[J]. Applied Energy, 2017, 195:234-246.

[22] Göbel J, Keeler H P, Krzesinski A E, et al. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay[J]. Performance Evaluation, 2016, 104:23–41.
[23] https://trustsql.qq.com/chain_oss/TrustSQL_WhitePaper.html
[24] George Hurlburt. Might the Blockchain Outlive Bitcoin?[M]. IT Professional,2016,18(2):12 –16.
[25] Janusz J. Blockchain technology in the chemical industry: Machine-to-machine electricity market [M]. Applied Energy,2017,195: 234-246.
[26] Aste T, Tasca P, Matteo T D. Blockchain Technologies: The Foreseeable Impact on Society and Industry[J]. Computer, 2017, 50(9):18-28.
[27] Wikipedia. Blockchain [EB/OL]. http://en.wikipedia.org/wiki/Blockchain,2015.
[28] Dorri A, Steger M, Kanhere S S, et al. BlockChain: A Distributed Solution to Automotive Security and Privacy[J]. IEEE Communications Magazine, 2017, 55(12):119-125.
[29] Berman P, Karpinski M, Nekrich Y. Optimal trade-off for Merkle tree traversal[J]. Theoretical Computer Science, 2011, 372(1):26-36.
[30] Delfs H, Knebl H. Public-Key Cryptography[M]. Introduction to Cryptography. Springer Berlin Heidelberg,2015:101-104.
[31] Saeki M. Elliptic Curve Cryptosystems[J]. Mathematics of Computation, 1997, 2(4):1024-1028.
[32] Filtz E, Polleres A, Karl R, et al. Evolution of the Bitcoin Address Graph[C]. International Data Science Conference.2017.
[33] Kosba A, Miller A. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]. 2016 IEEE SymPOSium on Security and Privacy, San Jose, California, USA,2016.
[34] Cusumano M A. The Bitcoin Ecosystem[J]. Communications of the Acm, 2014, 57(10):22-24.
[35] Narayanan A, Clark J. Bitcoin's Academic Pedigree[J]. Communications of the Acm, 2017, 60(12):36-45.
[36] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine Generals Problem [M]. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3):382–401.
[37] P. Koshy. Bitcoin and the Byzantine Generals Problem – a Crusade is needed A Revolution [EB/OL], http://financialcryptography.com/mt/archives/001522.html, 2014-10-19.
[38] Marshall Pease, Robert Shostak, and Leslie Lamport. Reaching agreement in the presence of faults [M]. Journal of the ACM (JACM),1980,27(2):228–234.
[39] Pierre-Louis Aublin, Sonia Ben Mokhtar, and Vivien Qu ema. RBFT: Redundant Byzantine Fault Tolerance[C], 2013 IEEE 33rd International Conference on Distributed Computing Systems (ICDCS), Philadelphia, Pennsylvania, USA,2013.
[40] D. Mazieres. The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus [EB/OL]. https://www.stellar.org/papers/stellar-consensus-protocol.pdf,2015-12-30.

[41] Richard Dennis; Gareth Owenson; Benjamin Aziz. A Temporal Blockchain: A Formal Analysis[C]. 2016 International Conference on Collaboration Technologies and Systems (CTS), Orlando, Florida, USA,2016.

[42] Forbes. Bitcoin: Whatever It Is, It's Not Money![J]. Communications of the Acm, 2013.

[43] 唐长兵,杨珍,郑忠龙,等.PoW 共识算法中的博弈困境分析与优化[J].自动化学报,2017,43(9):1520-1531.

[44] Peck M. A blockchain currency that beat s bitcoin on privacy [News][J]. IEEE Spectrum, 2016, 53(12):11-13.

[45] Bitcoin Wiki. Proof of Stake [EB/OL]. https://en.bitcoin.it/wiki/Proof_of_Stake,2015.

[46] Xia Q, Zhang F J, Zuo C. Review for Consensus Mechanism of Cryptocurrency System[J]. Computer Systems & Applications,2017.

[47] 黄秋波,安庆文,苏厚勤.一种改进 PBFT 算法作为以太坊共识机制的研究与实现[J].计算机应用与软件,2017(10).

[48] Kwon Y, Kim D, Son Y, et al. Doppelganger in Bitcoin Mining Pools: An Analysis of the Duplication Share Attack[C]// International Workshop on Information Security Applications. Springer, Cham,2016:124-135.

[49] Cawrey D. Are 51% attacks a real threat to bitcoin[J]. Coin Desk, June,2014, 20: 2014.

[50] Laszka A, Johnson B, Grossklags J. When Bitcoin Mining Pools Run Dry[M]. Financial Cryptography and Data Security. Springer Berlin Heidelberg,2015:63-77.

[51] Underwood S. Blockchain Beyond Bitcoin[J]. Communications of the Acm, 2016, 59(11):15-17.

[52] J. G?bel, A.E. Krzesinski, H.P. Keeler, et al. Bitcoin Blockchaindynamics: The selfish-mine strategy in the presence of propagation delay[J]. Performance Evaluation,2015, 104(1): 23-41.

攻读学位期间公开发表论文

[1] **Chaozhi Yang**, Tingting Cai, Zhihuai Li. Research on a tunable consistency strategy of the distributed database. International Conference on Information, Cybernetics and Computational Social Systems (ICCSS),2017,533-538. (EI: 20180304657083)

致　　谢

对于完成本次论文与实验我首先要感谢我的指导老师李老师和陈老师，没有他们的悉心指导，我就不会这么顺利的完成毕业论文。李老师把我们带到了新兴的区块链技术的大门前，为我们指引了一条的新的技术之路。陈老师从我们开题、中期一直到预答辩前都在帮我细心的审核论文。我在这里要郑重的向二位人类灵魂的工程师致敬。

随后我还有特别感谢陈同学和李同学，他们一同帮助我在实验室机房搭建了区块链网络环境，在我生病时帮我查看区块链网络运行是否正常。这份恩情我都会一直铭记于心，永远不忘掉。这里还要郑重鸣谢李同学为我的负载实验提供的比特币交易的数据集。我要感谢我的指导老师李志淮教授，从本科的毕业设计到研究生的毕业论文一直都悉心指导。

此外，实验室的其他师弟师妹们也在我的论文创作中提供了各种力所能及的帮助，特此感谢。

最后，对于各位老师在百忙之中为我审阅毕业论文感到由衷的感谢，希望各位老师不吝赐教、多提出一些建设性的问题。